VMware Horizon Client for Windows Installation and Setup Guide

VMware Horizon Client for Windows 2203

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware Horizon Client for Windows Installation and Setup Guide 6

1 System Requirements and Setup for Windows-Based Clients 7

Hardware and Software Requirements for Windows Client Systems 8

Smart Card Authentication Requirements 10

Client Device Certificate Authentication Requirements 12

OPSWAT Integration Requirements 12

System Requirements for Real-Time Audio-Video 13

System Requirements for Scanner Redirection 14

System Requirements for Serial Port Redirection 14

Requirements for Using URL Content Redirection 16

System Requirements for HTML5 Multimedia Redirection 16

System Requirements for Browser Redirection 17

System Requirements for Multimedia Redirection (MMR) 18

Configure E911 Services for Microsoft Teams 18

System Requirements for Geolocation Redirection 19

System Requirements for the Session Collaboration Feature 20

System Requirements for Skype for Business 21

Supported Desktop Operating Systems 21

2 Installing and Upgrading Horizon Client for Windows 22

Enabling FIPS Mode in the Windows Client Operating System 22

Enabling Automatic Internet Protocol Selection 23

Install Horizon Client for Windows 24

Install Horizon Client From the Command Line 26

Verify URL Content Redirection Installation 31

Update Horizon Client Online 32

3 Configuring Horizon Client for End Users 34

Preparing Connection Server for Horizon Client 34

Common Configuration Settings 37

Using URIs to Configure Horizon Client 37

Setting the Certificate Checking Mode in Horizon Client 45

Configuring the Certificate Checking Mode for End Users 47

Configuring Advanced TLS Options 48

Customizing the Horizon Client Menus 48

Customizing the Horizon Client Error Messages 49

Configuring Cursor Event Handling 49

Using Group Policy Settings to Configure Horizon Client 50
Running Horizon Client From the Command Line 80
Using the Windows Registry to Configure Horizon Client 86
Clearing the Last User Name Used to Log In to a Server 88
Configure VMware Blast Options 89
Using Internet Explorer Proxy Settings 91
Configure Horizon Client Data Sharing 91
MAC Address Deny List 93

4 Managing Remote Desktop and Published Application Connections 95
Connect to a Remote Desktop or Published Application 95
Use Unauthenticated Access to Connect to Published Applications 98
Share Location Information 100
Hide the VMware Horizon Client Window 101
Reconnecting to a Remote Desktop or Published Application 101
Create a Shortcut on the Windows Client Desktop or in the Start Menu 102
Configure Start Menu Shortcut Updates 102
Configure the Autoconnect Feature for a Remote Desktop 104
Log Off or Disconnect 104
Disconnecting From a Server 106

5 Working in a Remote Desktop or Published Application 107
Feature Support for Windows Clients 108
Resizing the Remote Desktop Window 109
Supported Multiple Monitor Configurations 110
Select Specific Monitors to Display a Remote Desktop 111
Display a Remote Desktop on a Single Monitor in a Multiple-Monitor Setup 112
Select Specific Monitors to Display Published Applications 113
Use Display Scaling 114
Using DPI Synchronization 115
Change the Display Mode for a Remote Desktop 116
Customize the Display Resolution and Display Scaling for a Remote Desktop 117
Use USB Devices 118
USB Redirection Limitations 121
Using Webcams and Microphones 122
When You Can Use a Webcam with the Real-Time Audio-Video Feature 122
Select a Preferred Webcam or Microphone on a Windows Client System 123
Using Multiple Devices with the Real-Time Audio-Video Feature 124
Select a Preferred Speaker for a Remote Desktop 125
Sharing Remote Desktop Sessions 125
Invite a User to Join a Remote Desktop Session 126

Manage a Shared Remote Desktop Session 128
Join a Remote Desktop Session 129
Share Local Folders and Drives 130
Open Local Files in Published Applications 133
Copying and Pasting 134
Logging Copy and Paste Activity 135
Configuring the Client Clipboard Memory Size 136
Dragging and Dropping 137
Tips for Using Published Applications 139
Reconnect to Published Applications After Disconnecting 140
Use Multiple Sessions of a Published Application From Different Client Devices 141
Use a Local IME with Published Applications 141
Use a Local IME with a Remote Desktop 143
Printing From a Remote Desktop or Published Application 144
Set Printing Preferences for the VMware Integrated Printing Feature 144
Printing From a Remote Desktop to a Local USB Printer 145
Improve Mouse Performance in a Remote Desktop 146
Using Scanners 146
Redirecting Serial Ports 148
Keyboard Shortcuts for Input Focus 150
Keyboard Input Source Language Synchronization 150
Configure Lock Key Synchronization 150

6 Troubleshooting Horizon Client 152
Restart a Remote Desktop 152
Reset Remote Desktops or Published Applications 153
Repair Horizon Client for Windows 154
Uninstall Horizon Client for Windows 155
Problems with Keyboard Input 155
What to Do If Horizon Client Quits Unexpectedly 156
Connecting to a Server in Workspace ONE Mode 156

VMware Horizon Client for Windows Installation and Setup Guide

This guide describes how to install, configure, and use VMware Horizon® Client™ software on a Microsoft Windows client system.

This information is intended for administrators who need to set up a Horizon deployment that includes Microsoft Windows client systems, such as desktops and laptops. The information is written for experienced system administrators who are familiar with virtual machine technology and data center operations.

If you are an end user, see the *VMware Horizon Client for Windows User Guide* document, or view the Horizon Client for Windows online help.

System Requirements and Setup for Windows-Based Clients

1

Systems that run Horizon Client components must meet certain hardware and software requirements.

Horizon Client on Windows systems uses Microsoft Internet Explorer Internet settings, including proxy settings, when connecting to a server. Ensure that your Internet Explorer settings are accurate and that you can access the server URL through Internet Explorer.

This chapter includes the following topics:

- Hardware and Software Requirements for Windows Client Systems
- Smart Card Authentication Requirements
- Client Device Certificate Authentication Requirements
- OPSWAT Integration Requirements
- System Requirements for Real-Time Audio-Video
- System Requirements for Scanner Redirection
- System Requirements for Serial Port Redirection
- Requirements for Using URL Content Redirection
- System Requirements for HTML5 Multimedia Redirection
- System Requirements for Browser Redirection
- System Requirements for Multimedia Redirection (MMR)
- Configure E911 Services for Microsoft Teams
- System Requirements for Geolocation Redirection
- System Requirements for the Session Collaboration Feature
- System Requirements for Skype for Business
- Supported Desktop Operating Systems

Hardware and Software Requirements for Windows Client Systems

You can install Horizon Client for Windows on PCs and laptops that use a supported Microsoft Windows operating system.

The PC or laptop on which you install Horizon Client, and the peripherals it uses, must meet certain system requirements.

Models

All x86-64 Windows devices

Memory

At least 1 GB of RAM

Operating systems

Horizon Client supports the following operating systems.

OS	Version	Service Pack or Servicing Option	Supported Editions
Windows 11	64-bit	N/A	Home, Pro, Pro for Workstations, Enterprise, Internet of Things (IoT) Enterprise, and Education
Windows 10	64-bit	Version 21H2 SAC Version 21H1 SAC Version 20H2 SAC Enterprise 2021 LTSC Enterprise 2019 LTSC	Home, Pro, Pro for Workstations, Enterprise, Internet of Things (IoT) Enterprise, and Education
Windows Server 2012 R2	64-bit	Latest update	Standard and Datacenter
Windows Server 2016	64-bit	Latest update	Standard and Datacenter
Windows Server 2019	64-bit	Latest update	Standard and Datacenter

Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019 are supported for the purposes of running Horizon Client in nested mode. For information about the features that are supported in nested mode, see VMware Knowledge Base (KB) article 67248.

Important Sometimes, new Windows operating systems are supported after this document is published. For the most up-to-date operating system support information, see VMware Knowledge Base (KB) article 58096.

Connection Server and Horizon Agent

Latest maintenance release of Horizon 7 version 7.5 and later releases.

If client systems connect from outside the corporate firewall, use a Unified Access Gateway appliance so that client systems do not require a VPN connection. If your company has an internal wireless network to provide routable access to remote desktops that devices can use, you do not need to set up Unified Access Gateway or a VPN connection.

Display protocols

- PCoIP
- VMware Blast
- RDP

Network protocols

- IPv4
- IPv6

During a custom Horizon Client installation, you can enable the automatic selection of the Internet protocol. For more information, see Enabling Automatic Internet Protocol Selection. For information about using Horizon in an IPv6 environment, see the *Horizon Installation* document.

Hardware requirements for PCoIP and VMware Blast

- x86-based processor with SSE2 extensions, with an 800 MHz or faster processor speed.
- Available RAM above system requirements to support various monitor setups. Use the following formula as a general guide. The unit of measurement is pixels.

  ```
  20 MB + (24 * (# monitors) * (monitor width) * (monitor height))
  ```

  In general, you can use the following calculations.

  ```
  1 monitor: 1600 x 1200: 64 MB
  2 monitors: 1600 x 1200: 128 MB
  3 monitors: 1600 x 1200: 256 MB
  ```

Hardware requirements for RDP

- x86-based processor with SSE2 extensions, with an 800 MHz or faster processor speed.
- 128 MB RAM.

Software requirements for RDP

- For Windows 10, use RDP 10.0.
- The agent installer configures the local firewall rule for inbound RDP connections to match the current RDP port of the host operating system, which is typically 3389. If you change the RDP port number, you must change the associated firewall rules.

You can download Remote Desktop Client versions from the Microsoft Download Center.

Video and graphics requirements

- Graphics card that supports Direct3D 11 Video.
- Latest video and graphics card drivers.

.NET Framework requirements

The Horizon Client installer requires .NET Framework version 4.5 or later. The installer checks whether .NET Framework version 4.5 or later is installed before installation. If the client machine does not meet this prerequisite, the installer downloads the latest version of .NET Framework automatically.

To use Horizon Client, .NET Desktop Runtime for Windows x86 version 5.0 or later is required. The Horizon Client installer installs a recent version of Desktop Runtime. After you install Horizon Client, you can update Desktop Runtime from https://dotnet.microsoft.com/download/dotnet/5.0/runtime.

Smart Card Authentication Requirements

Client devices that use a smart card for user authentication must meet certain requirements.

Client Hardware and Software Requirements

Each client device that uses a smart card for user authentication must have the following hardware and software.

- Horizon Client
- Smart cards and smart card readers that use a PKCS#11 or Microsoft CNG API/CryptoAPI provider.
- Product-specific application drivers

Users that authenticate with smart cards must have a smart card or USB smart card token, and each smart card must contain a user certificate.

Before issuing a certificate, you must create the certificate template. You must select either **Key Storage Provider** or **Legacy Cryptographic Service Provider**.

To create a KSP certificate template, select **Windows Server 2008** or later for the Certification Authority on the **Compatibility** tab and select **Key Storage Provider** on the **Cryptography** tab.

If you are using a KSP certificate template to issue the certificate, for the CSP specified in the certificate issuing template, select **Microsoft Smart Card Key Storage Provider** or a third-party smart card KSP that supports RSA with SHA-256 algorithms. If you are using a legacy CSP certificate template, select **Microsoft Base Smart Card Crypto Provider** or a third-party smart card CSP that supports RSA with SHA-256 algorithms.

Smart Card Enrollment Requirements

To install certificates on a smart card, an administrator must set up a computer to act as an enrollment station. This computer must have the authority to issue smart card certificates for users, and it must be a member of the domain for which you are issuing certificates.

When you enroll a smart card, you can select the key size of the resulting certificate. To use smart cards with local desktops, you must select a 1024-bit or 2048-bit key size when you enroll the smart card. Certificates that have 512-bit keys are not supported.

The Microsoft TechNet website includes detailed information about planning and implementing smart card authentication for Windows systems.

Remote Desktop and Published Application Software Requirements

A Horizon administrator must install product-specific application drivers on the virtual desktops or RDS host.

Enabling the User Name Hint Text Box in Horizon Client

In some environments, smart card users can use a single smart card certificate to authenticate to multiple user accounts. Users enter their user name in the **Username hint** text box when they sign in with a smart card.

To make the **Username hint** text box appear on the Horizon Client login dialog box, you must enable the smart card user name hints feature in Connection Server. For information about enabling the smart card user name hints feature, see the *Horizon Administration* document.

If your environment uses a Unified Access Gateway appliance for secure external access, you must configure the Unified Access Gateway appliance to support the smart card user name hints feature. The smart card user name hints feature is supported only with Unified Access Gateway 2.7.2 and later. For information about enabling the smart card user name hints feature in Unified Access Gateway, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Horizon Client continues to support single-account smart card certificates even when the smart card user name hints feature is enabled.

Additional Smart Card Authentication Requirements

In addition to meeting the smart card requirements for Horizon Client systems, other Horizon components must meet certain configuration requirements to support smart cards.

Connection Server and security server hosts

An administrator must add all applicable Certificate Authority (CA) certificate chains for all trusted user certificates to a server truststore file on the Connection Server host or, if a security server is used, on the security server host. These certificate chains include root certificates and, if an intermediate certificate authority issues the user's smart card certificate, must also include intermediate certificates.

For information about configuring Connection Server to support smart card use, see the *Horizon Administration* document.

Unified Access Gateway appliances

For information about configuring smart card authentication on a Unified Access Gateway appliance, see the *Deploying and Configuring VMware Unified Access Gateway* document.

Active Directory

For information about tasks that an administrator might need to perform in Active Directory to implement smart card authentication, see the *Horizon Administration* document.

Client Device Certificate Authentication Requirements

With the client device certificate authentication feature, you can set up certificate authentication for client devices. Unified Access Gateway authenticates the client devices. Microsoft Certificate Services, with Active Directory, manages the creation and distribution of certificates to the client devices. After successful device authentication, the user must still perform user authentication.

This feature has the following requirements.

- Unified Access Gateway 2.6 or later
- Horizon 7 version 7.5 or later
- A certificate installed on the client device that Unified Access Gateway accepts

For information about configuring Unified Access Gateway, see the Unified Access Gateway documentation.

Before issuing a certificate, you must create the certificate template. You must select either **Key Storage Provider** or **Legacy Cryptographic Service Provider**.

To create a KSP certificate template, select **Windows Server 2008** or later for the Certification Authority on the **Compatibility** tab and select **Key Storage Provider** on the **Cryptography** tab.

If you are using a KSP certificate template to issue the certificate, select **Microsoft Software Key Storage Provider** or a third-party smart card KSP that supports RSA with SHA-256 algorithms. If you are using a legacy CSP certificate template, select **Microsoft Enhanced RSA and AES Cryptographic Provider**, which supports RSA with SHA-256 algorithms and TLS1.2.

For a list of CryptoAPI cryptographic service providers, go to https://docs.microsoft.com/en-us/windows/win32/seccertenroll/cryptoapi-cryptographic-service-providers.

OPSWAT Integration Requirements

At some companies, an administrator might integrate Unified Access Gateway with the third-party OPSWAT MetaAccess application. This integration, which is typically used on unmanaged devices in corporate bring-your-own-device (BYOD) environments, enables organizations to define device acceptance policies for Horizon Client devices.

For example, an administrator might define a device acceptance policy that requires client devices to be password protected or have a minimum operating system version. Client devices that comply with the device acceptance policy can access remote desktops and published applications through Unified Access Gateway. Unified Access Gateway denies access to remote resources from client devices that do not comply with the device acceptance policy.

Normally, applications downloaded from Unified Access Gateway are run on the client in the context of the user. This behaviour can be changed by setting a flag on Unified Access Gateway as documented below. The default flag is `RUN_AS_USER`.

	Description	
Flag	**User has admin Rights**	**User does not have admin Rights**
`RUN_AS_USER`	Run in the user context. Do not copy code to the client install path.	Run in the user context. Do not copy code to the client install path.
`RUN_AS_USER_IF_ADMIN`	Run in the user context. Do not copy code to the client install path.	Do not run.
`RUN_AS_USER_IF_NON_ADMIN`	Do not run.	Run in the user context. Do not copy code to the client install path.
`RUN_AS_SYSTEM`	Run in the system context, including copying code to the client install path.	Run in the system context, including copying code to the client install path.
`RUN_AS_SYSTEM_IF_ADMIN`	Run in the system context, including copying code to the client install path.	Do not run.

For more information, see the *Deploying and Configuring VMware Unified Access Gateway* document.

System Requirements for Real-Time Audio-Video

Real-Time Audio-Video works with standard webcam, USB audio, and analog audio devices. The feature also works with standard conferencing applications. To support Real-Time Audio-Video, your Horizon deployment must meet certain software and hardware requirements.

Virtual desktops

To use more than one webcam or microphone in a virtual desktop, Horizon Agent 7.10 or later must be installed.

When using Microsoft Teams with Real-Time Audio-Video, virtual desktops must have a minimum of 4 vCPUs and 4 GB of RAM.

Horizon Client computer or client access device

- Real-Time Audio-Video is supported on all operating systems that run Horizon Client for Windows. For information, see Hardware and Software Requirements for Windows Client Systems.

- The webcam and audio device drivers must be installed, and the webcam and audio device must be operable, on the client computer. You do not need to install the device drivers on the machine where the agent is installed.

Display protocols

- PCoIP
- VMware Blast

System Requirements for Scanner Redirection

End users can scan information into their remote desktops and applications with scanners that are connected to their local client systems. To use this feature, the remote desktops and client computers must meet certain system requirements.

Remote desktops

Remote desktops must have Horizon Agent installed with the Scanner Redirection setup option selected on the parent or template virtual machines or RDS hosts. On Windows desktop and Windows Server guest operating systems, the Horizon Agent Scanner Redirection setup option is deselected by default.

For information about which guest operating systems are supported for virtual desktops and RDS hosts, and for information about configuring scanner redirection in remote desktops and published applications, see "Configure Scanner Redirection" in the *Configuring Remote Desktop Features in Horizon* document.

Horizon Client computer or client access device

Scanner redirection is supported on Windows 10. The scanner device drivers must be installed, and the scanner must be operable, on the client computer. You do not need to install the scanner device drivers on the remote desktop operating system where the agent is installed.

Scanning device standard

TWAIN or WIA

Display protocols

- PCoIP
- VMware Blast

Scanner redirection is not supported in RDP desktop sessions.

System Requirements for Serial Port Redirection

With the serial port redirection feature, end users can redirect locally connected serial (COM) ports, such as built-in RS232 ports or USB to Serial adapters, to their remote desktops and published applications. To support serial port redirection, your VMware Horizon deployment must meet certain software and hardware requirements.

Virtual desktops

Horizon Agent must be installed with the Serial Port Redirection setup option selected. This setup option is deselected by default.

The following operating systems are supported on virtual desktops.

- 64-bit Windows 7
- 64-bit Windows 8.x
- 64-bit Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note Horizon Agent 2006 and later does not support Windows 7, Windows 8.x, Window Server 2008 R2, and Windows Server 2012 R2.

Serial port device drivers do not need to be installed in the virtual desktop.

Published desktops and published applications

RDS hosts must have Horizon Agent 7.6 or later installed with the Serial Port Redirection setup option selected. This setup option is deselected by default.

The following operating systems are supported for published desktops and published applications.

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note Horizon Agent 2006 and later does not support Windows Server 2008 R2 and Windows Server 2012 R2.

Serial port device drivers do not need to be installed in the RDS host.

Serial port redirection is available with full desktops and not supported on published applications on RDS hosts.

Horizon Client computer or client access device

Serial port redirection is supported on Windows 10 client systems. Any required serial port device drivers must be installed and the serial port must be operable.

Display protocols

- PCoIP
- VMware Blast

Serial port redirection is not supported in RDP desktop sessions.

For information about configuring serial port redirection, see "Configuring Serial Port Redirection" in the *Configuring Remote Desktop Features in Horizon* document.

Requirements for Using URL Content Redirection

With the URL Content Redirection feature, URL content can be redirected from the client machine to a remote desktop or published application (client-to-agent redirection), or from a remote desktop or published application to the client machine (agent-to-client redirection).

For example, an end user can click a link in the native Microsoft Word application on the client and the link opens in the remote Internet Explorer application, or an end user can click a link in the remote Internet Explorer application and the link opens in a native browser on the client machine. Any number of protocols can be configured for redirection, including HTTP, mailto, and callto.

A Horizon administrator must also configure settings that specify how Horizon Client redirects URL content from the client to a remote desktop or published application, or how Horizon Agent redirects URL content from a remote desktop or published application to the client.

For complete information, see the "Configuring URL Content Redirection" topic in the *Configuring Remote Desktop Features in Horizon* document.

System Requirements for HTML5 Multimedia Redirection

Horizon Agent and Horizon Client, and the remote desktops and client systems on which you install the agent and client software, must meet certain requirements to support the HTML5 Multimedia Redirection feature.

With HTML5 Multimedia Redirection, if an end user uses the Google Chrome or Microsoft Edge browser in a remote desktop, HTML5 multimedia content is sent to the client system. The client system plays the multimedia content, which reduces the load on the ESXi host, and the end user has a better audio and video experience.

Remote desktop

- Horizon Agent must be installed on the virtual desktop or RDS host for published desktops with the HTML5 Multimedia Redirection custom setup option selected. Beginning with

Horizon Agent 7.10, the HTML5 Multimedia Redirection custom setup option is removed and HTML5 Multimedia Redirection is installed by default. For more information, see the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.

- The HTML5 Multimedia Redirection group policy settings must be configured on the Active Directory server. See the topics about configuring HTML5 Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon* document.
- The Google Chrome, Microsoft Edge, or Microsoft Edge (Chromium) browser must be installed.
- The VMware Horizon HTML5 Multimedia Redirection extension must be installed in the browser. See the topics about configuring HTML5 Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon* document.

Client system

- The Support for HTML5 Multimedia Redirection and Browser Redirection custom setup option must be selected when you install Horizon Client. This option is selected by default.

Display protocol for the remote session

- PCoIP
- VMware Blast

TCP port

HTML5 Multimedia Redirection uses port 9427.

System Requirements for Browser Redirection

The remote desktops and client systems on which you install the agent and client software must meet certain requirements to support the Browser Redirection feature.

With Browser Redirection, when an end user opens a website in the Chrome browser in a remote desktop, the web page is rendered on the client system instead of the agent system, and it is displayed over the remote browser's viewport. The viewport is the portion of the browser window that contains the content of the web page.

Remote desktops

- Horizon Agent 7.10 or later must be installed on the virtual desktop or RDS host for published desktops. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.
- The VMware Browser Redirection group policy settings must be configured on the Active Directory server. See the topics about configuring Browser Redirection in the *Configuring Remote Desktop Features in Horizon* document.

- The Chrome browser or Microsoft Edge (Chromium) browser must be installed.
- The VMware Horizon Browser Redirection extension must be installed in the browser. See the topics about configuring Browser Redirection in the *Configuring Remote Desktop Features in Horizon* document.

Display protocol for the remote session

- PCoIP
- VMware Blast

System Requirements for Multimedia Redirection (MMR)

With multimedia redirection (MMR), the multimedia stream is decoded on the client system. The client system plays the media content so that the load on the ESXi host is reduced.

Remote desktops

For information about operating system requirements and other software requirements and configuration settings, see the topics about Windows Media Multimedia Redirection in the *Configuring Remote Desktop Features in Horizon* document.

Horizon Client computer or client access device

Windows 10

Supported media formats

Media formats that Windows Media Player supports, for example: M4V; MOV; MP4; MPEG-4 Part 2; WMV 7, 8, and 9; WMA; AVI; ACE; MP3.

MP3 is not supported when using MMS and RTSP.

Note DRM-protected content is not redirected through Windows Media MMR.

Configure E911 Services for Microsoft Teams

To allow E911 services for the Media Optimization for Microsoft Teams feature, you must manually enable Windows location services for Horizon Client. These services provide the client's geolocation information to Microsoft Teams running in a remote desktop for location-based routing during emergency calls.

Note E911 services require Horizon Agent 2111 or later.

To enable location services for Horizon Client on Windows, follow the steps below.

1. In the Settings dialog box, navigate to **Privacy & Security**.
2. Under App permissions, click **Location** tab.
3. Set **Location services** to **On**.

4 Set **Let apps access your location** to **On**.

System Requirements for Geolocation Redirection

Horizon Agent and Horizon Client, and the virtual desktop or RDS host and client machine on which you install the agent and client software, must meet certain requirements to support the Geolocation Redirection feature.

The source of the geolocation information is the operating system of the local device using Horizon Client. This information can be redirected by the client to remote desktops or published applications. The configuration settings of the host system and the agent can restrict the feature's availability.

With Geolocation Redirection, geolocation information is sent from the client system to the remote desktop or published application.

Virtual desktop or RDS host

- The Windows **Location service** setting must be **On** in **Settings > Privacy > Location**.
- The Geolocation Redirection feature supports the following remote desktop applications.

Application	Platform
Google Chrome (latest version)	All virtual desktops or RDS hosts
Internet Explorer 11	All virtual desktops or RDS hosts
Microsoft Edge (Chromium)	All virtual desktops or RDS hosts
Microsoft Edge, Maps, Weather, and other Win32 and UWP apps	Windows 10

  The **Location** permission setting, if any, must be enabled individually in each supported browser.
- Horizon Agent 7.6 or later must be installed with the Geolocation Redirection custom setup option selected. This option is not selected by default. See the topics about installing Horizon Agent in the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.
- The VMware Geolocation Redirection group policy settings must be configured on the Active Directory server. See the topics about configuring Geolocation Redirection in the *Configuring Remote Desktop Features in Horizon* document.
- For Internet Explorer 11, the VMware Horizon Gelocation IE Plugin must be enabled for RDS hosts. You do not need to enable the VMware Horizon Geolocation Redirection IE plugin for Windows 10 virtual desktops. Internet Explorer is supported on Windows 10 virtual desktops with the VMware Geolocation Redirection driver. See the topics about configuring Geolocation Redirection in the *Configuring Remote Desktop Features in Horizon* document.

- For Chrome and Microsoft Edge (Chromium), the VMware Horizon Geolocation Redirection Chrome extension must be installed. See the topics about configuring Geolocation Redirection in the *Configuring Remote Desktop Features in Horizon* document.

Client system

- To share the client system's location information, you must configure the **Geolocation** settings in Horizon Client.

Display protocol for the remote session

- Horizon Client for Windows - PCoIP or VMware Blast

System Requirements for the Session Collaboration Feature

With the Session Collaboration feature, users can invite other users to join an existing remote desktop session. To support the Session Collaboration feature, your Horizon deployment must meet certain requirements.

Session collaborators

To join a collaborative session, a user must have Horizon Client for Windows, Mac, or Linux installed on the client system, or must use HTML Access.

Windows remote desktops

The Session Collaboration feature must be enabled at the desktop pool or farm level. For information about enabling the Session Collaboration feature for desktop pools, see the *Setting Up Virtual Desktops in Horizon* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon* document.

You can use Horizon Agent group policy settings to configure the Session Collaboration feature. For information, see the *Configuring Remote Desktop Features in Horizon* document.

Linux remote desktops

For Linux remote desktop requirements, see the *Setting Up Linux Desktops in Horizon* document.

Connection Server

The Session Collaboration feature requires that the Connection Server instance uses an Enterprise license.

Display protocols

VMware Blast

The Session Collaboration feature does not support published application sessions.

System Requirements for Skype for Business

An end user can run Skype for Business inside a virtual desktop without negatively affecting the virtual infrastructure and overloading the network. During Skype audio and video calls, all media processing takes place on the client machine instead of in the virtual desktop.

To use this feature, you must install the Virtualization Pack for Skype for Business feature on the client machine when Horizon Client for Windows is installed. For information, see Chapter 2 Installing and Upgrading Horizon Client for Windows.

A Horizon administrator must also install the VMware Virtualization Pack for Skype for Business feature on the virtual desktop when Horizon Agent is installed. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon* document.

For complete requirements, see "Configure Skype for Business" in the *Configuring Remote Desktop Features in Horizon* document.

Supported Desktop Operating Systems

A Horizon administrator creates virtual machines that have a guest operating system and installs agent software in the guest operating system. End users can log in to these virtual machines from a client device.

For a list of the supported Windows guest operating systems, see the *Horizon Installation* document.

Some Linux guest operating systems are also supported. For information about system requirements, configuring Linux virtual machines, and a list of supported features, see the *Setting Up Linux Desktops in Horizon* document.

Installing and Upgrading Horizon Client for Windows

2

You can obtain the Windows-based Horizon Client installer from the VMware website, or from a Web access page provided by Connection Server. You can set various startup options for end users after Horizon Client is installed. You can update Horizon Client online.

This chapter includes the following topics:

- Enabling FIPS Mode in the Windows Client Operating System
- Enabling Automatic Internet Protocol Selection
- Install Horizon Client for Windows
- Install Horizon Client From the Command Line
- Verify URL Content Redirection Installation
- Update Horizon Client Online

Enabling FIPS Mode in the Windows Client Operating System

If you plan to install Horizon Client with Federal Information Processing Standard (FIPS) compliant cryptography, you must enable FIPS mode in the client operating system before you run the Horizon Client installer.

When FIPS mode is enabled in the client operating system, applications use only cryptographic algorithms that are FIPS-140 compliant and in compliance with FIPS-approved modes of operation. You can enable FIPS mode by enabling a specific security setting, either in the Local Security Policy or as part of Group Policy, or by editing a Windows Registry key.

For more information about FIPS compliance, see the *Horizon Installation* document.

Setting the FIPS Configuration Property

To enable FIPS mode in the client operating system, you can use a Windows group policy setting or a Windows Registry setting for the client computer.

- To use the group policy setting, open the Group Policy Editor, navigate to `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options`, and enable the **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** setting.
- To use the Windows Registry, go to `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` and set **Enabled** to 1.

For more information about FIPS mode, go to https://support.microsoft.com/en-us/kb/811833.

Important If you do not enable FIPS mode before running the Horizon Client installer, the installer option to use FIPS-compliant cryptography does not appear during a custom installation. FIPS-compliant cryptography is not enabled during a typical installation. If you install Horizon Client without the FIPS-compliant cryptography option and you later decide to use the option, you must uninstall the client, enable FIPS mode in the client operating system, and run the Horizon Client installer again.

Enabling Automatic Internet Protocol Selection

When you perform a custom installation of Horizon Client, you can enable the automatic selection of the Internet protocol. With automatic selection, Horizon Client checks the current network and connects over IPv4 or IPv6 automatically.

When automatic selection is enabled, the following features are supported with Unified Access Gateway 3.3 and later with the VMware Blast display protocol.

- Log in as current user
- Audio-out
- Customer Experience Improvement Program data collection
- Virtual Printing
- VMware Integrated Printing (requires Horizon 7 version 7.7 or later)
- HTML5 Multimedia Redirection
- VMware video
- USB redirection
- Real-Time Audio-Video (RTAV)

Install Horizon Client for Windows

You can run a Windows-based installer file to install all Horizon Client components.

This procedure describes how to install Horizon Client by using an interactive installation wizard. To install Horizon Client from the command line, see Install Horizon Client From the Command Line. To install the URL Content Redirection feature, you must run the installer from the command line.

Note You can install Horizon Client in the remote desktop virtual machine. Companies might use this installation strategy when their end users access published applications from Windows thin-client devices.

Prerequisites

- Verify that the client system uses a supported operating system. See Hardware and Software Requirements for Windows Client Systems.
- Verify that you have the URL for a download page that contains the Horizon Client installer. This URL might be the VMware Downloads page at http://www.vmware.com/go/viewclients, or it might be the URL for a Connection Server instance.
- Verify that you can log in as an administrator on the client system.
- Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other.
- If you plan to install Horizon Client with FIPS-compliant cryptography, enable FIPS mode in the client operating system. See Enabling FIPS Mode in the Windows Client Operating System.
- If you plan to select the IPv6 protocol or automatic Internet protocol selection, see the *Horizon Installation* document for information about features that are not available in an IPv6 environment.
- If you plan to enable automatic Internet protocol selection, see Enabling Automatic Internet Protocol Selection for information about the supported features.
- If you plan to install the **USB Redirection** component, perform the following tasks:
  - Determine whether the person who uses the client device is allowed to access locally connected USB devices from a remote desktop. If access is not permitted, either do not install the **USB Redirection** component, or install the component and disable it by using a group policy setting. If you use group policy to disable USB redirection, you do not need to reinstall Horizon Client if you later decide to enable USB redirection for a client. For more information, see Using Group Policy Settings to Configure Horizon Client.
  - Verify that the Windows Automatic Update feature is not turned off on the client computer.
- Decide whether to use the feature that allows end users to log in to Horizon Client and their remote desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. Some client operating systems do not support this feature.

- If you do not want end users to have to supply the fully qualified domain name (FQDN) of the Connection Server instance, determine the FQDN so that you can supply it during installation.

Procedure

1 Log in to the client system as an administrator.

2 Navigate to the VMware Downloads page at http://www.vmware.com/go/viewclients.

3 Download the installer file, for example, `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

YYMM is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

4 Double-click the installer file to begin the installation.

5 Select an installation type and follow the prompts.

Option	Action
Typical installation	Click **Agree & Install**. The installer configures the client to use the IPv4 Internet protocol and installs the following features. ■ USB Redirection ■ Log in as current user, including showing the **Log in as current user** menu option. ■ Virtualization Pack for Skype for Business ■ Support for HTML5 Multimedia Redirection and Browser Redirection ■ Media Optimization for Microsoft Teams
Custom installation	Click **Customize Installation** and select the features to install. You must select this option to install the following features. ■ Specify a non-default installation location. ■ Use the IPv6 Internet protocol or automatic selection. If you enable automatic selection, Horizon Client checks the current network and connects over IPv4 or IPv6 automatically. ■ Set the default login behavior to **Log in as current user**. ■ Specify a default Connection Server instance. ■ Enable FIPS-compliant cryptography. FIPS-compliant cryptography custom installation options are available in the installer only if FIPS mode is enabled on the client operating system. ■ Select **Enable Keylogger Blocking** to enable the anti keylogger feature.

Results

Some features require you to restart the client system.

The installer installs Windows services, including VMware Horizon Client (`horizon_client_service`) and VMware USB Arbitration Service (`VMUSBArbService`).

What to do next

Start Horizon Client and verify that you can log in to the correct remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Install Horizon Client From the Command Line

You can install Horizon Client from the command line by typing the installer filename and specifying installation commands and properties. You can install Horizon Client silently from the command line.

The following table describes the Horizon Client installation commands.

Table 2-1. Horizon Client Installation Commands

Command	Description
`/?` or `/help`	Lists the Horizon Client installation commands and properties.
`/silent`	Installs Horizon Client silently. You do not need to respond to wizard prompts.
`/install`	Installs Horizon Client interactively. You must respond to wizard prompts.
`/uninstall`	Uninstalls Horizon Client.
`/repair`	Repairs Horizon Client.
`/norestart`	Suppresses all restarts and restart prompts during the installation process.
`/x /extract`	Extracts the installer packages into the `%TEMP%` directory.
`/l` or `/log`	Specifies a folder and a naming pattern for installation log files. For example, if you specify the following command, the Horizon Client installer creates log files that have the prefix `Test` in the folder named `C:\Temp`. `/log "C:\Temp\Test"`

The following table describes the Horizon Client installation properties.

Table 2-2. Horizon Client Installation Properties

Property	Description	Default
`INSTALLDIR`	Path and folder in which Horizon Client is installed. For example: `INSTALLDIR=""D:\abc\my folder""` The sets of double quotes that enclose the path enable the installer to interpret the space as a valid part of the path.	`%ProgramFiles%VMware \VMware Horizon View Client`
`VDM_IP_PROTOCOL_USAGE`	IP (Internet Protocol) version that Horizon Client components use for communication. Valid values are as follows: ■ IPv4 ■ IPv6 ■ Dual If you specify Dual, Horizon Client checks the current network and connects over IPv4 or IPv6 automatically.	IPv4
`VDM_FIPS_ENABLED`	Determines whether to install Horizon Client with FIPS-compliant cryptography. A value of 1 installs Horizon Client with FIPS-compliant cryptography. A value of 0 installs Horizon Client without FIPs-compliant cryptography. **Note** Before you set this property to 1, you must enable FIPS mode in the Windows client operating system. See Enabling FIPS Mode in the Windows Client Operating System.	0
`VDM_SERVER`	Fully qualified domain name (FQDN) of the Connection Server instance to which Horizon Client users connect by default. For example: `VDM_Server=cs1.companydomain.com` If you configure this property, Horizon Client users do not need to supply this FQDN.	None
`LOGINASCURRENTUSER_DISPLAY`	Determines whether **Log in as current user** appears in the **Options** menu on the Horizon Client menu bar. Valid values are 1 (enabled) or 0 (disabled).	1

Table 2-2. Horizon Client Installation Properties (continued)

Property	Description	Default
`LOGINASCURRENTUSER_DEFAULT`	Determines whether **Log in as current user** is selected by default in the **Options** menu on the Horizon Client menu bar. Valid values are 1 (enabled) and 0 (disabled). When log in as current user is the default login behavior, the identity and credential information that users provide when they log in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. When log in as current user is not the default login behavior, users must provide identity and credential information multiple times before they can access a remote desktop or application. **Note** If you change this value for the user interface, Horizon Client ignores the related default group policy setting.	0
`ADDLOCAL`	Specifies the features to install. Valid values are as follows: ■ `ALL` - Installs all available features, except for URL Content Redirection. ■ `TSSO` - Installs the Log in as Current User feature. ■ `USB` - Installs the USB Redirection feature. To specify individual features, enter a comma-separated list of feature names. Do not use spaces between names. For example, to install Horizon Client with the USB Redirection feature, but without the Log in as Current User feature, type the following command: `VMware-Horizon-Client-`*`y.y.y-xxxxxx`*`.exe ADDLOCAL=USB`	None
`INSTALL_SFB`	Determines whether the VMware Virtualization Pack for Skype for Business feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature.	1
`INSTALL_HTML5MMR`	Determines whether the Support for HTML5 Multimedia Redirection and Browser Redirection feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature.	1

Table 2-2. Horizon Client Installation Properties (continued)

Property	Description	Default
`REMOVE`	Specifies the features not to install. Valid values are as follows: ■ `Scanner` - Does not install the scanner redirection feature. ■ `FolderRedirection` - Does not install the folder redirection feature. ■ `SerialPort` - Does not install the serial port redirection feature. To specify multiple features, enter a comma-separated list of feature names. Do not use spaces between names. For example, the following command does not install the scanner redirection feature: `VMware-Horizon-Client-`*`y.y.y-xxxxxx`*`.exe REMOVE=Scanner`	None
`DESKTOP_SHORTCUT`	Determines whether to create a desktop shortcut for Horizon Client. A value of 0 does not create a desktop shortcut. A value of 1 creates a desktop shortcut.	1
`STARTMENU_SHORTCUT`	Determines whether to create a Start menu shortcut for Horizon Client. A value of 0 does not create a Start menu shortcut. A value of 1 creates a Start menu shortcut.	1
`URL_FILTERING_ENABLED`	Determines whether the URL Content Redirection feature is installed. A value of 1 installs the feature. A value of 0 does not install the feature. When you set this property to 1 in an interactive installation, the **URL Content Redirection** check box appears under Additional features on the custom installation dialog box and is selected by default. The check box does not appear unless you set this property to 1. **Note** The `ADDLOCAL=ALL` property does not include the URL Content Redirection feature.	0
`AUTO_UPDATE_ENABLED`	Determines whether the online update feature is enabled. A value of 1 enables the feature. A value of 0 disables the feature. For more information, see Update Horizon Client Online.	1

Table 2-2. Horizon Client Installation Properties (continued)

Property	Description	Default
`INSTALL_TEAMS_REDIRECTION`	Determines whether the Media Optimization for Microsoft Teams feature is enabled. A value of 1 enables the feature. A value of 0 disables the feature. For more information about this feature, see the *Configuring Remote Desktop Features in Horizon* document.	1
`KEYLOGGER_BLOCKING_ENABLED`	Determines whether keylogger blocking is enabled. A value of 1 enables the feature. A value of 0 disables the feature. The feature is disabled by default.	

Prerequisites

- Verify that the client system uses a supported operating system. See Hardware and Software Requirements for Windows Client Systems.
- Verify that you can log in as an administrator on the client system.
- Verify that the domain controllers have the latest patches, enough free disk space, and can communicate with each other.
- If you plan to install Horizon Client with FIPS-compliant cryptography, enable FIPS mode in the client operating system. See Enabling FIPS Mode in the Windows Client Operating System.
- Decide whether to use the feature that allows end users to log in to Horizon Client and their remote desktop as the currently logged in user. Credential information that the user entered when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop. Some client operating systems do not support this feature.
- Become familiar with the Horizon Client installation commands.
- Become familiar with the Horizon Client installation properties.
- Determine whether to allow end users to access locally connected USB devices from their remote desktops. If not, set the `ADDLOCAL` installation property to the list of features and omit the USB feature.
- If you do not want end users to have to supply the fully qualified domain name (FQDN) of the Connection Server instance, determine the FQDN so that you can supply it during installation.

Procedure

1. Log in to the client system as an administrator.
2. Navigate to the VMware Downloads page at http://www.vmware.com/go/viewclients.

3 Download the Horizon Client installer file, for example, `VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe`.

   YYMM is the marketing version number, *y.y.y* is the internal version number, and *xxxxxx* is the build number.

4 Open a command prompt on the Windows client computer.

5 Type the installer file name, installation commands, and installation properties on one line.

   `VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe [commands] [properties]`

Results

The installer installs Horizon Client according to the installation commands and properties that you specify. If you specify the `/silent` installation command, the wizard prompts do not appear.

The installer installs Windows services, including VMware Horizon Client (`horizon_client_service`) and VMware USB Arbitration Service (`VMUSBArbService`).

Example: Sample Installation Commands

The following command installs Horizon Client interactively and enables the URL Content Redirection feature.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

The following command installs Horizon Client silently and suppresses all restarts and restart prompts during the installation process.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe /silent /norestart
```

What to do next

If you enabled the URL Content Redirection feature when you installed Horizon Client, verify that the feature is installed. See Verify URL Content Redirection Installation.

Start Horizon Client and verify that you can log in to the correct remote desktop or published application. See Connect to a Remote Desktop or Published Application.

Verify URL Content Redirection Installation

If you enabled the URL Content Redirection feature when you installed Horizon Client, verify that the feature was installed.

Prerequisites

Specify the `URL_FILTERING_ENABLED=1` installation property when you install Horizon Client. See Install Horizon Client From the Command Line.

Procedure

1. Log in to the client machine.
2. Verify that the `vmware-url-protocol-launch-helper.exe` and `vmware-url-filtering-plugin.dll` files are installed in the `%PROGRAMFILES%\VMware\VMware Horizon View Client\` directory.
3. Verify that the VMware Horizon View URL Filtering Plugin add-on is installed and enabled in Internet Explorer.

Update Horizon Client Online

You can update Horizon Client online.

By default, a green icon appears on the **Options** menu to indicate that a new Horizon Client version is available.

During the update process, by default, you can select or deselect the **Check for updates and show badge notification** check box to specify whether Horizon Client checks for updates automatically and displays the new version notification.

You can control the behavior of the online update feature by configuring the following group policy settings.

- **Enable Horizon Client online update**, which enables or disables the online update feature.
- **URL for Horizon Client online update**, which specifies an alternate URL from which Horizon Client can retrieve updates.
- **Automatically check for update**, which controls the **Check for updates and show badge notification** check box.
- **Update message pop-up**, which controls the **Show pop-up message when there is an update** check box. The **Show pop-up message when there is an update** check box takes effect only if the **Check for updates and show badge notification** check box is selected.
- **Allow user to skip Horizon Client update**, which controls the **Skip** button.

For complete information about these group policy settings, see Using Group Policy Settings to Configure Horizon Client.

You can also disable the online update feature by setting the `AUTO_UPDATE_ENABLED` property to 0 when you install Horizon Client from the command line. For more information, see Install Horizon Client From the Command Line.

Prerequisites

- Save your work before you update Horizon Client. The update might initiate a system reboot.
- Verify that you can log in as an administrator on the client system.

Procedure

1 Log in to the client system as an administrator.

2 Start Horizon Client, click **Options** in the menu bar and select **Software Updates**.

3 To check for available updates, click **Check for Updates**.

   Horizon Client indicates whether an update is available.

4 To begin the update process if a new version is available, click **Download and Install**.

   Alternatively, you can click **Skip** (if available), or click **Remind Me Later** to install the update another time. If you click **Skip**, you do not see another update notification until the next Horizon Client version is available. You can still click **Software Updates** to manually check for an update.

5 To install the update after Horizon Client has downloaded it, click **OK**.

   The Horizon Client interactive installation wizard opens.

Configuring Horizon Client for End Users

3

Configuring Horizon Client for end users can involve configuring URIs to start Horizon Client, configuring the certificate checking mode, setting advanced TLS options, customizing the Horizon Client menus, and using group policies to configure custom settings.

This chapter includes the following topics:

- Preparing Connection Server for Horizon Client
- Common Configuration Settings
- Using URIs to Configure Horizon Client
- Setting the Certificate Checking Mode in Horizon Client
- Configuring the Certificate Checking Mode for End Users
- Configuring Advanced TLS Options
- Customizing the Horizon Client Menus
- Customizing the Horizon Client Error Messages
- Configuring Cursor Event Handling
- Using Group Policy Settings to Configure Horizon Client
- Running Horizon Client From the Command Line
- Using the Windows Registry to Configure Horizon Client
- Clearing the Last User Name Used to Log In to a Server
- Configure VMware Blast Options
- Using Internet Explorer Proxy Settings
- Configure Horizon Client Data Sharing
- MAC Address Deny List

Preparing Connection Server for Horizon Client

Before end users can connect to a server and access a remote desktop or published application, a Horizon administrator must configure certain Connection Server settings.

Unified Access Gateway and Security Servers

If your VMware Horizon deployment includes a Unified Access Gateway appliance, configure Connection Server to work with Unified Access Gateway. See the *Deploying and Configuring VMware Unified Access Gateway* document. Unified Access Gateway appliances perform the same role as security servers.

If your VMware Horizon deployment includes a security server, verify that you are using the latest maintenance releases of Connection Server 7.5 and Security Server 7.5 or later releases. For more information, see the installation document for your Horizon version.

Note Security servers are not supported in VMware Horizon 2006 and later.

Secure Tunnel Connection

If you plan to use a secure tunnel connection for client devices, and if the secure connection is configured with a DNS host name for a Connection Server instance or a security server, verify that the client device can resolve this DNS name. .

Desktop and Application Pools

Use the following check list when configuring desktop and application pools.

- Verify that a desktop or application pool has been created and that the user account that you plan to use is entitled to access the pool. For more information, see the *Setting Up Virtual Desktops in Horizon* and *Setting Up Published Desktops and Applications in Horizon* documents.
- If end users have a high-resolution display and use the **High Resolution Mode** client setting while viewing their remote desktops in full-screen mode, verify that sufficient vRAM is allocated for each Windows remote desktop. The amount of vRAM depends on the display resolution and the number of monitors configured for end users.

User Authentication

Use the following check list when setting up user authentication.

- To provide end users with unauthenticated access to published applications in Horizon Client, you must enable this feature in the Connection Server instance. For more information, see the topics about unauthenticated access in the *Horizon Administration* document.
- To use two-factor authentication, such as RSA SecurID or RADIUS authentication, with Horizon Client, you must enable the two-factor authentication feature for the Connection Server instance. Beginning with Horizon 7 version 7.11, you can customize the labels on the RADIUS authentication login page. Beginning with Horizon 7 version 7.12, you can configure two-factor authentication to occur after a remote session times out. For more information, see the topics about two-factor authentication in the *Horizon Administration* document.

- To allow the Connection Server instance to accept the user identity and credential information that is passed when users select **Log in As Current User** from the **Options** menu in Horizon Client menu bar, enable the **Accept logon as current user** setting for the Connection Server instance. This setting is available in Horizon 7 version 7.8 and later. For more information, see the *Horizon Administration* document.

  You can use Horizon Client group policy settings to configure the Log in as current user feature, including specifying a list of Connection Server instances that can accept Log in as current user authentication information. For information about these client-side settings, see Using Group Policy Settings to Configure Horizon Client.
- To hide the server URL in Horizon Client, enable the **Hide server information in client user interface** global setting. For more information, see the *Horizon Administration* document.
- To hide the **Domain** drop-down menu in Horizon Client, enable the **Hide domain list in client user interface** global setting. Beginning with Horizon 7 version 7.8, this setting is enabled by default. For more information, see the *Horizon Administration* document.
- To send the domain list to Horizon Client, enable the **Send domain list** global setting in Horizon Console. This setting is available in Horizon 7 version 7.8 and later and is deactivated by default. Earlier Horizon 7 versions send the domain list. For more information, see the *Horizon Administration* document.

The following table shows how the **Send domain list** and **Hide domain list in client user interface** global settings determine how users can log in to the server.

Send domain list setting	Hide domain list in client user interface setting	How users log in
Disabled (default)	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. - User name (not allowed for multiple domains) - ***domain\username*** - ***username@domain.com***
Disabled (default)	Disabled	If a default domain is configured on the client, the default domain appears in the **Domain** drop-down menu. If the client does not know a default domain, `*DefaultDomain*` appears in the **Domain** drop-down menu. Users must enter one of the following values in the **User name** text box. - User name (not allowed for multiple domains) - ***domain\username*** - ***username@domain.com***

Send domain list setting	Hide domain list in client user interface setting	How users log in
Enabled	Enabled	The **Domain** drop-down menu is hidden. Users must enter one of the following values in the **User name** text box. ■ User name (not allowed for multiple domains) ■ ***domain\username*** ■ ***username@domain.com***
Enabled	Disabled	Users can enter a user name in the **User name** text box and then select a domain from the **Domain** drop-down menu. Alternatively, users can enter one of the following values in the **User name** text box. ■ ***domain\username*** ■ ***username@domain.com***

Common Configuration Settings

Horizon Client provides several configuration mechanisms that simplify the login and remote desktop selection experience for end users, and enforce security policies.

The following table shows only some of the configuration settings that you can set in one or more ways.

Table 3-1. Common Configuration Settings

Setting	Mechanisms for Configuring
Server address	URI, Group Policy, Command Line, Windows Registry
Active Directory user name	URI, Group Policy, Command Line, Windows Registry
Domain name	URI, Group Policy, Command Line, Windows Registry
Remote desktop display name	URI, Group Policy, Command Line
Window size	URI, Group Policy, Command Line
Display protocol	URI, Command Line
Configuring certificate checking	Group Policy, Windows Registry
Configuring TLS protocols and cryptographic algorithms	Group Policy, Windows Registry

Using URIs to Configure Horizon Client

You can use uniform resource identifiers (URIs) to create web page or email links that end users can click to start Horizon Client, connect to a server, or open a remote desktop or published application.

You create these links by constructing URIs that provide some or all the following information, so that your end users do not need to supply it.

- Server address
- Port number for the server
- Active Directory user name
- RADIUS or RSA SecurID user name, if different from the Active Directory user name
- Domain name
- Remote desktop or published application display name
- Window size
- Actions including reset, log out, and start session
- Display protocol
- Options for redirecting USB devices

To construct a URI, you use the `vmware-view` URI scheme with Horizon Client specific path and query parts.

To use URIs to start Horizon Client, Horizon Client must already be installed on client computers.

Syntax for Creating vmware-view URIs

URI syntax includes the `vmware-view` URI scheme, a path part to specify the remote desktop or published application, and, optionally, a query to specify remote desktop or published application actions or configuration options.

URI Specification

Use the following syntax to create URIs to start Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

The only required element is the URI scheme, `vmware-view`. Because the scheme name is case-sensitive for some versions of some client operating systems, type `vmware-view`.

Important In all parts, non-ASCII characters must first be encoded according to UTF-8 [STD63], and then each octet of the corresponding UTF-8 sequence must be percent-encoded to be represented as URI characters.

For information about encoding for ASCII characters, see the URL encoding reference at http://www.utf8-chartable.de/.

authority-part

The server address and, optionally, a user name, a non-default port number, or both. Underscores (_) are not supported in server names. Server names must conform to DNS syntax.

To specify a user name, use the following syntax.

```
user1@server-address
```

You cannot specify a UPN address, which includes the domain. To specify the domain, you can use the `domainName` query part in the URI.

To specify a port number, use the following syntax.

```
server-address:port-number
```

path-part

The display name of the remote desktop or published application. The display name is specified in Horizon Console when the desktop pool or application pool is created. If the display name contains a space, use the **%20** encoding mechanism to represent the space.

Alternatively, you can specify a desktop or application ID, which is a path string that includes the desktop or application pool ID. To find a desktop or application ID, open ADSI Edit on the Connection Server host, navigate to `DC=vdi,dc=vmware,dc=int`, and select the `OU=Applications` node. All the desktop and application pools are listed. The `distinguishedName` attribute specifies the ID value. You must encode the ID value before you specify it in a URI, for example, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

If you specify a desktop or application ID, you must use only lowercase letters, even if the desktop or application ID contains uppercase letters in ADSI Edit.

Note More than one remote desktop or published application can have the same display name, but the desktop and application ID is unique. To specify a particular remote desktop or published application, use the desktop or application ID rather than the display name.

query-part

The configuration options to use, or the remote desktop or published application actions to perform. Queries are not case-sensitive. To use multiple queries, use an ampersand (&) between the queries. If the queries conflict, Horizon Client uses the last query in the list. Use the following syntax.

```
query1=value1[&query2=value2...]
```

Supported Queries

The following queries are supported for this type of Horizon Client. If you are creating URIs for multiple types of clients, such as desktop clients and mobile clients, see the installation and setup guide for each type of client system for the list of supported queries.

action

Table 3-2. Values That Can Be Used with the action Query

Value	Description
`browse`	Displays a list of available remote desktops and published applications hosted on the specified server. You are not required to specify a remote desktop or published application when using this action.
`start-session`	Opens the specified remote desktop or published application. If no action query is provided and the remote desktop or published application name is provided, `start-session` is the default action.
`reset`	Shuts down and restarts the specified remote desktop or published application. Unsaved data is lost. Resetting a remote desktop is the same as pressing the Reset button on a physical PC.
`restart`	Shuts down and restarts the specified remote desktop. Restarting a remote desktop is the same as the Windows operating system restart command. The operating system usually prompts the user to save any unsaved data before it restarts.
`logoff`	Logs the user out of the guest operating system in the remote desktop. If you specify a published application, the action is ignored or the end user sees the warning message "Invalid URI action."

args

Specifies command-line arguments to add when the published application starts. Use the syntax `args=`*value*, where *value* is a string. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**
- For a double quotation mark ("), use **`%22`**

For example, to specify the filename `"My new file.txt"` for the Notepad++ application, use **`%22My%20new%20file.txt%22`**.

appProtocol

For published applications, valid values are **`PCOIP`** and **`BLAST`**. For example, to specify PCoIP, use the syntax **`appProtocol=PCOIP`**.

connectUSBOnInsert

Connects a USB device to the foreground remote desktop or published application when you plug in the device. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redirects all USB devices that are currently connected to the client system to the remote desktop or published application. This query is implicitly set if you specify the `unattended` query for a remote desktop. To use this query, you must set the `action` query to **`start-session`** or else not have an `action` query. Valid values are **`true`** and **`false`**. An example of the syntax is **`connectUSBOnStartup=true`**.

desktopLayout

Sets the size of the remote desktop window. To use this query, you must set the `action` query to **`start-session`** or not have an `action` query.

Table 3-3. Valid Values for the desktopLayout Query

Value	Description
`fullscreen`	Full screen on one monitor. This value is the default.
`multimonitor`	Full screen on all monitors.
`windowLarge`	Large window.
`windowSmall`	Small window.
*W*x*H*	Custom resolution, where you specify the width by height, in pixels. An example of the syntax is **`desktopLayout=1280x800`**.

desktopProtocol

For remote desktops, valid values are **`RDP`**, **`PCOIP`**, and **`BLAST`**. For example, to specify PCoIP, use the syntax **`desktopProtocol=PCOIP`**.

domainName

Specifies the NETBIOS domain name associated with the user who is connecting to the remote desktop or published application. For example, you might use `mycompany` rather than `mycompany.com`.

filePath

Specifies the path to the file on the local system that you want to open with the published application. You must specify the full path, including the drive letter. Use percent encoding for the following characters:

- For a colon (:), use **`%3A`**
- For a back slash (\), use **`%5C`**
- For a space ( ), use **`%20`**

For example, to represent file path `C:\test file.txt`, use **`C%3A%5Ctest%20file.txt`**.

launchMinimized

Starts Horizon Client in minimized mode. Horizon Client remains minimized until the specified remote desktop or published application starts. The syntax is **`launchMinimized=true`**. You cannot use this query with the **unattended** query.

tokenUserName

Specifies the RSA or RADIUS user name. Use this query only if the RSA or RADIUS user name is different from the Active Directory user name. If you do not specify this query and RSA or RADIUS authentication is required, Horizon Client uses the Windows user name. The syntax is **`tokenUserName=`*`name`***.

unattended

Creates a server connection to a remote desktop in kiosk mode. If you use this query, do not specify user information if you generated the account name from the MAC address of the client device. If you created custom account names in ADAM, such as names that begin with "custom-", you must specify the account information.

useExisting

If this option is set to **`true`**, only one Horizon Client instance can run. If users try to connect to a second server, they must log out of the first server, causing remote desktop and published application sessions to be disconnected. If this option is set to **`false`**, multiple Horizon Client instances can run and users can connect to multiple servers at the same time. The default is **`true`**. An example of the syntax is **`useExisting=false`**.

unauthenticatedAccessEnabled

If this option is set to **`true`**, the Unauthenticated Access feature is enabled by default. The **Unauthenticated Access** option is visible in the user interface and is selected. If this option is set to **`false`**, the Unauthenticated Access feature is deactivated. The **Unauthenticated Access** setting is hidden and deactivated. When this option is set to **`""`**, the Unauthenticated Access feature is deactivated and the **Unauthenticated Access** setting is hidden from the user interface and deactivated. An example of the syntax is **`unauthenticatedAccessEnabled=true`**.

unauthenticatedAccessAccount

If the Unauthenticated Access feature is enabled, sets the account to use. If Unauthenticated Access is deactivated, then this query is ignored. An example of the syntax using the **`anonymous1`** user account is **`unauthenticatedAccessAccount=anonymous1`**.

Examples of vmware-view URIs

You can use the `vmware-view` URI scheme to create hypertext links or buttons and include these links in email or on a Web page. For example, an end user can click a URI link to start a remote desktop with the startup options that you specify.

Each URI example is followed by a description of what the end user sees after clicking the URI link.

1

```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the display name `Primary Desktop`, and the user is logged in to the guest operating system.

Note In this example, the default display protocol and window size are used. The default display protocol is PCoIP and the default window size is full screen.

2

```
vmware-view://view.mycompany.com/
cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint
```

Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, the client connects to the remote desktop that has the desktop ID `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (encoded value `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3

```
vmware-view://view.mycompany.com:7555/Primary%20Desktop
```

This URI has the same effect as the previous example, except that it uses the nondefault port of 7555 for the Connection Server instance. (The default port is 443.) Because a remote desktop identifier is provided, the remote desktop opens, even though the `start-session` action is not included in the URI.

4

```
vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP
```

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`. The user must supply the domain name and password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system. The connection uses the PCoIP display protocol.

5

```
vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST
```

Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the user must supply the user name, domain name, and password. After a successful login, the client connects to the published application that has the display name `Calculator`. The connection uses the VMware Blast display protocol.

6.
   ```
   vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany
   ```

   Horizon Client starts and connects to the `view.mycompany.com` server. In the login dialog box, the **User name** text box is populated with `fred`, and the **Domain** text box is populated with `mycompany`. The user must supply only a password. After a successful login, the client connects to the remote desktop that has the display name `Finance Desktop`, and the user is logged in to the guest operating system.

7.
   ```
   vmware-view://view.mycompany.com/
   ```

   Horizon Client starts and the user is taken to the login prompt for connecting to the `view.mycompany.com` server.

8.
   ```
   vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
   ```

   Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client resets the specified desktop.

   Note This action is available only if a Horizon administrator has enabled the reset feature for the remote desktop.

9.
   ```
   vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
   ```

   Horizon Client starts and connects to the `view.mycompany.com` server. The login dialog box prompts the user for a user name, domain name, and password. After a successful login, Horizon Client restarts the specified desktop.

   Note This action is available only if a Horizon administrator has enabled the restart feature for the remote desktop.

10.
   ```
   vmware-view://view.mycompany.com/Primary%20Desktop?action=start-
   session&connectUSBOnStartup=true
   ```

   This URI has the same effect as the first example, and all USB devices connected to the client system are redirected to the remote desktop.

11.
   ```
   vmware-view://
   ```

   If Horizon Client is not running, it starts. If Horizon Client is already running, it comes to the foreground.

12.
   ```
   vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
   ```

   Starts My Notepad++ on server 10.10.10.10 and passes the argument `My new file.txt` in the published application start command. Spaces and double quotes use percent escaping. The filename is enclosed in double quotes because it contains spaces.

You can also type this command at the Windows command-line prompt by using the following syntax:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

In this example, double quotes are escaped by using the characters \".

13

```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Starts Notepad++ 12 on server 10.10.10.10 and passes the argument `a.text b.txt` in the published application start command. Because the argument is not enclosed in quotes, a space separates the filenames and the two files are opened separately in Notepad++.

Note Published applications can differ in the way that they use command-line arguments. For example, if you pass the argument `a.txt b.txt` to WordPad, WordPad opens only one file, `a.txt`.

14

```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client starts and connects to the `view.mycompany.com` server using the **`anonymous1`** user account. The Notepad application starts without prompting the user to provide login credentials.

HTML Code Examples

You can use URIs to make hypertext links and buttons to include in emails or on Web pages. The following examples show how to use the URI from the first URI example to code the hypertext link labeled **Test Link** and a button labeled **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</
a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Setting the Certificate Checking Mode in Horizon Client

Server certificate checking occurs for connections between Horizon Client and a server. A certificate is a digital form of identification, similar to a passport or a driver's license.

Server certificate checking includes the following checks:

- Has the certificate been revoked?

- Is the certificate intended for a purpose other than verifying the identity of the sender and encrypting server communications? That is, is it the correct type of certificate?
- Has the certificate expired, or is it valid only in the future? That is, is the certificate valid according to the computer clock?
- Does the common name on the certificate match the host name of the server that sends it? A mismatch can occur if a load balancer redirects Horizon Client to a server that has a certificate that does not match the host name entered in Horizon Client. Another reason a mismatch can occur is if you enter an IP address rather than a host name in the client.
- Is the certificate signed by an unknown or untrusted certificate authority (CA)? Self-signed certificates are one type of untrusted CA. To pass this check, the certificate's chain of trust must be rooted in the device's local certificate store.

For information about distributing a self-signed root certificate to all Windows client systems in a domain, see "Add the Root Certificate to Trusted Root Certification Authorities" in the *Horizon Installation* document.

To set the certificate checking mode, start Horizon Client and select **Settings > Security**. You can select one of the following options. Note that you cannot configure certificate checking in FIPS mode.

- **Never connect to untrusted servers**. This setting means that you cannot connect to the server if any of the certificate checks fail. An error message lists the checks that failed.
- **Warn before connecting to untrusted servers**. This setting means that you can click **Continue** to ignore the warning if a certificate check fails because the server uses a self-signed certificate. For self-signed certificates, the certificate name is not required to match the server name that you entered in Horizon Client. You can also receive a warning if the certificate has expired.
- **Do not verify server identity certificates**. This setting means that no certificate checking occurs.

If an administrator later installs a security certificate from a trusted certificate authority and all certificate checks pass when you connect, this trusted connection is remembered for that specific server. In the future, if that server ever presents a self-signed certificate again, the connection fails. After a particular server presents a fully verifiable certificate, it must always do so.

Important If you previously used group policy to configure your company's client systems to use a specific cipher, such as by configuring SSL Cipher Suite Order group policy settings, you must now use a Horizon Client group policy security setting. See Using Group Policy Settings to Configure Horizon Client. Alternatively, you can use the `SSLCipherList` registry setting on the client system. See Using the Windows Registry to Configure Horizon Client.

You can configure the default certificate checking mode and prevent end users from changing it in Horizon Client. For more information, see Configuring the Certificate Checking Mode for End Users.

Using an SSL Proxy Server

If you use an SSL proxy server to inspect traffic sent from the client environment to the Internet, enable the **Allow connection via an SSL Proxy** setting. This setting allows certificate checking for secondary connections through an SSL proxy server and applies to both Blast Secure Gateway and secure tunnel connections. If you use an SSL proxy server and enable certificate checking, but you do not enable the **Allow connection via an SSL Proxy** setting, connections fail because of mismatched thumbprints. The **Allow connection via an SSL Proxy** setting is not available if you enable the **Do not verify server identity certificates** option. When the **Do not verify server identity certificates** option is enabled, Horizon Client does not verify the certificate or thumbprint and an SSL proxy is always allowed.

You can use the **Configures the SSL Proxy certificate checking behavior of the Horizon Client** group policy setting to configure whether to allow certificate checking for secondary connections through an SSL proxy server. For more information, see Using Group Policy Settings to Configure Horizon Client.

To allow VMware Blast connections through a proxy server, see Configure VMware Blast Options.

Configuring the Certificate Checking Mode for End Users

You can configure the certificate checking mode for end users. For example, you can configure that full verification is always performed. Certificate checking occurs for TLS connections between a server and Horizon Client.

You can configure one of the following certificate verification strategies for end users.

- End users are allowed to select the certificate checking mode in Horizon Client.
- (No verification) No certificate checks are performed.
- (Warn) If the server presents a self-signed certificate, end users are warned. Users can determine whether to allow this type of connection.
- (Full security) Full verification is performed and connections that do not pass full verification are rejected.

If you use an SSL proxy server to inspect traffic sent from the client environment to the Internet, you can configure certificate checking for secondary connections through the SSL proxy server. This feature applies to both Blast Secure Gateway and secure tunnel connections. You can also allow proxy server use for VMware Blast connections.

For information about the types of certificate checks that can be performed, see Setting the Certificate Checking Mode in Horizon Client.

You can use Horizon Client group policy settings to set the certificate checking mode, allow SSL proxy use, restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted TLS connection, and enable proxy use for VMware Blast connections. For more information, see Using Group Policy Settings to Configure Horizon Client.

If you do not want to configure the certificate checking mode as a group policy, you can enable certificate checking by adding the `CertCheckMode` value name to one of the following registry keys on the client computer:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- For 64-bit Windows: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware VDM\Client\Security`

Use the following values in the registry key:

- **0** implements `Do not verify server identity certificates.`
- **1** implements `Warn before connecting to untrusted servers.`
- **2** implements `Never connect to untrusted servers.`

If you configure both the group policy setting and the `CertCheckMode` setting in the registry key, the group policy setting takes precedence over the registry key value.

Configuring Advanced TLS Options

You can select the security protocols and cryptographic algorithms that are used to encrypt communications between Horizon Client and servers, and between Horizon Client and the agent in a remote desktop.

These security options are also used to encrypt the USB channel.

With the default setting, cipher suites use 128-bit or 256-bit AES, remove anonymous DH algorithms, and then sort the current cipher list in order of encryption algorithm key length.

By default, TLS v1.1 and TLS v1.2 are enabled. SSL v2.0, SSL v3.0, and TLS v1.0 are not supported.

If you configure a security protocol for Horizon Client that is not enabled on the server to which the client connects, a TLS error occurs and the connection fails.

Important At least one of the protocols that you enable in Horizon Client must also be enabled on the remote desktop or USB devices cannot be redirected to the remote desktop.

On the client system, you can use either a group policy setting or a Windows Registry setting to change the default ciphers and protocols. For information about using a group policy setting, see the **Configures SSL protocols and cryptographic algorithms** setting in Using Group Policy Settings to Configure Horizon Client. For information about using the SSLCipherList setting in the Windows Registry, see Using the Windows Registry to Configure Horizon Client.

Customizing the Horizon Client Menus

You can use Horizon Client group policies to hide some items in certain menus in the Horizon Client user interface.

For information about using the group policies that control the Horizon Client menus, see the descriptions of the **Hide items in application context menu**, **Hide items in desktop context menu**, **Hide items in desktop toolbar**, **Hide items in system tray menu**, and **Hide items in the client toolbar menu** group policy settings in Using Group Policy Settings to Configure Horizon Client.

Customizing the Horizon Client Error Messages

You can use the Horizon Client **Custom error screen footer** group policy setting to add custom help text to the bottom of all error messages that appear in the Horizon Client user interface. For example, your help text might tell users how to contact the help desk at your company.

You must create a plain text (`.txt`) file on the local client system to contain the help text. The text file can contain up to 2048 characters, including control characters. Both ANSI and Unicode encoding are supported. You specify the full path to this text file when you configure the **Custom error screen footer** group policy setting.

For detailed information about using the **Custom error screen footer** group policy setting, see Using Group Policy Settings to Configure Horizon Client.

Configuring Cursor Event Handling

You can optimize cursor event handling by configuring settings in the `C:\ProgramData\VMware\VMware Horizon View\config.ini` file on the Windows client system.

Note To use cursor event handling, Horizon Agent 2006 or later must be installed on the remote desktop.

Setting	Description
`RemoteDisplay.allowCursorWarping`	Enables or disables the cursor warping feature. When this feature is enabled and the mouse is in absolute mode, the remote agent detects sudden cursor movements and reflects them to the client by moving the local cursor. When this feature is disabled, the client ignores sudden cursor movements in the remote agent. Valid values are TRUE or FALSE. The default value is TRUE.
`RemoteDisplay.allowCursorEventsOnLowLatencyChannel`	Determines whether the low-latency channel is used for cursor updates. Valid values are TRUE or FALSE. The default value is TRUE.

You can configure the maximum latency allowed when coalescing mouse movements by setting the **Configure maximum latency for mouse coalescing** group policy setting. For more information, see Using Group Policy Settings to Configure Horizon Client.

You can also configure cursor event handling on the agent machine. For example, you can use the agent-side **Cursor Warping** group policy setting to configure cursor warping, and you can modify Windows registry settings on the agent machine to enable or disable coalescing mouse movement events and the low-latency channel. The settings on both the client and agent must match for the feature to be enabled. For information about the agent-side settings, see the *Configuring Remote Desktop Features in Horizon* document.

Using Group Policy Settings to Configure Horizon Client

Horizon Client includes a group policy ADMX template file that you can use to configure Horizon Client features and behavior. You can optimize and secure remote desktop and published application connections by adding the policy settings in the ADMX template file to a new or existing GPO in Active Directory.

The template file contains both Computer Configuration and User Configuration group policies.

- The Computer Configuration policies set policies that apply to Horizon Client, regardless of who is running the client on the host.
- The User Configuration policies set Horizon Client policies that apply to all users who are running Horizon Client, and to RDP connection settings. User Configuration policies override equivalent Computer Configuration policies.

Horizon Client applies policies when remote desktops and published applications start and when users log in.

The Horizon Client Configuration ADMX template file (`vdm_client.admx`), and all ADMX template files that provide group policy settings, are available in `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, where *YYMM* is the marketing version number, *x.x.x* is the internal version number, and *yyyyyyy* is the build number. You can download this ZIP file from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. You must copy the file to your Active Directory server and use the Group Policy Management Editor to add the administrative templates. For instructions, see the *Configuring Remote Desktop Features in Horizon* document.

Scripting Definition Settings for Client GPOs

You can set group policies for many of the same settings that you can configure when you run Horizon Client from the command line, including the remote desktop window size, login user name, and login domain name.

The following table describes the scripting definition settings in the VMware Horizon Client Configuration ADMX template file. This template file provides a Computer Configuration and a User Configuration version of each scripting definition setting. The User Configuration setting overrides the equivalent Computer Configuration setting. The settings appear in the **VMware Horizon Client Configuration > Scripting definitions** folder in Group Policy Management Editor.

Table 3-4. VMware Horizon Client Configuration Template: Scripting Definitions

Setting	Description
`Automatically connect if only one launch item is entitled`	If a user is entitled to only one remote desktop, connect the user to that remote desktop. This setting prevents the user from having to select a remote desktop from a list that contains only one remote desktop.
`Connect all USB devices to the desktop or remote application on launch`	Determines whether all the available USB devices on the client system are connected to the remote desktop or published application when the remote desktop or published application starts.
`Connect USB devices to the desktop or remote application when they are plugged in`	Determines whether USB devices are connected to the remote desktop or published application when the devices are plugged in to the client system.
`DesktopLayout`	Specifies the layout of the Horizon Client window that users see when they log into a remote desktop. The layout choices are as follows: - `Full Screen` - `Multimonitor` - `Window - Large` - `Window - Small` This setting is available only when the `DesktopName to select setting` is also set.
`DesktopName to select`	Specifies the default remote desktop that Horizon Client uses during login.
`Disable 3rd-party Terminal Services plugins`	Determines whether Horizon Client checks third-party Terminal Services plugins that are installed as normal RDP plugins. If you do not configure this setting, Horizon Client checks third-party plugins by default. This setting does not affect Horizon-specific plugins, such as USB redirection.
`Locked Guest Size`	If the display is used on one monitor, specifies the screen resolution of the remote desktop. This setting does not work if you set the remote desktop display to **All Monitors**. After you enable this setting, remote desktop autofit functionality is disabled and the **Allow Display Scaling** option is hidden in the Horizon Client user interface.
`Logon DomainName`	Specifies the NetBIOS domain that Horizon Client uses during login.
`Logon Password`	Specifies the password that Horizon Client uses during login. The password is stored in plain text by Active Directory. For improved security, do not specify this setting. Users can enter the password interactively.
`Logon UserName`	Specifies the password that Horizon Client uses during login. The password is stored in plain text by Active Directory.
`Server URL`	Specifies the URL that Horizon Client uses during login, for example, `https://view1.example.com`.

Table 3-4. VMware Horizon Client Configuration Template: Scripting Definitions (continued)

Setting	Description
`Suppress error messages (when fully scripted only)`	Determines whether Horizon Client error messages are hidden during login. This setting applies only when the login process is fully scripted, for example, when all the required login information is prepopulated through group policy. If the login fails because of incorrect login information, users are not notified and the Horizon Client process is terminated.
`Disconnected application session resumption behavior`	Determines how running published applications behave when users reconnect to a server. The choices are as follows: ■ Ask to reconnect to open applications ■ Reconnect automatically to open applications ■ Do not ask and do not automatically reconnect When this setting is enabled, end users cannot configure the published application reconnection behavior in Horizon Client. When this setting is disabled, end users can configure published application reconnection behavior in Horizon Client. This setting is disabled by default.
`Enable Unauthenticated Access to the server`	Determines whether users are required to enter credentials to access their published applications when they use Horizon Client. When this setting is enabled, the **Unauthenticated Access** setting in Horizon Client is visible, disabled, and selected. The client can fall back to another authentication method if Unauthenticated Access is not available. When this setting is disabled, users are always required to enter their credentials to log in and access their published applications. The **Unauthenticated Access** setting in Horizon Client is hidden and deselected. Users can enable Unauthenticated Access in Horizon Client by default. The **Unauthenticated Access** setting is visible, enabled, and deselected.
`Account to use for Unauthenticated Access`	Specifies the Unauthenticated Access user account that Horizon Client uses to log in anonymously to the server if the `Enable Unauthenticated Access to the server` group policy setting is enabled, or if a user enables Unauthenticated Access by selecting **Unauthenticated Access** in Horizon Client. If Unauthenticated Access is not used for a specific connection to a server, this setting is ignored. Users can select an account by default.
`Use existing client instance when connect to same server`	Determines whether a connection is added to the existing Horizon Client instance with which the user is already connected to the same server. This setting is disabled by default when not configured.

Security Settings for Client GPOs

Security settings include group policies for certificates, login credentials, and the single sign-on feature.

The following table describes the security settings in the Horizon Client Configuration ADMX template file. This table shows whether the settings include both Computer Configuration and User Configuration settings, or only Computer Configuration settings. For the security settings that include both types of settings, the User Configuration setting overrides the equivalent Computer Configuration setting. These settings appear in the **VMware Horizon Client Configuration > Security Settings** folder in the Group Policy Management Editor.

Table 3-5. Horizon Client Configuration Template: Security Settings

Setting	Computer	User	Description
`Allow command line credentials`	X		Determines whether user credentials can be provided with Horizon Client command-line options. If this setting is disabled, the `smartCardPIN` and `password` options are not available when users run Horizon Client from the command line. This setting is enabled by default. The equivalent Windows Registry value is `AllowCmdLineCredentials`.
`Configures the SSL Proxy certificate checking behavior of the Horizon Client`	X		Determines whether to allow certificate checking for secondary connections through an SSL proxy server for Blast Secure Gateway and secure tunnel connections. When this setting is not configured (the default), users can change the SSL proxy setting in Horizon Client manually. See Setting the Certificate Checking Mode in Horizon Client. By default, Horizon Client blocks SSL proxy connections for Blast Secure Gateway and secure tunnel connections.
`Servers Trusted For Delegation`	X		Specifies the Connection Server instances that accept the user identity and credential information that is passed when a user selects **Log in as current user** in the **Options** menu on the Horizon Client menu bar. If you do not specify any Connection Server instances, all Connection Server instances accept this information, unless the **Allow logon as current user** authentication setting is disabled for the Connection Server instance in Horizon Console. To add a Connection Server instance, use one of the following formats: ■ `domain\system$` ■ `system$@domain.com` ■ The Service Principal Name (SPN) of the Connection Server service. The equivalent Windows Registry value is `BrokersTrustedForDelegation`.

Table 3-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Computer	User	Description
`Certificate verification mode`	X		Configures the level of certificate checking that Horizon Client performs. You can select one of these modes: ■ `No Security`. No certificate checking occurs. ■ `Warn But Allow`. If a certificate check fails because the server uses a self-signed certificate, users see a warning, which they can ignore. For self-signed certificates, the certificate name is not required to match the server name that users enter in Horizon Client. If any other certificate error condition occurs, Horizon Client shows an error and prevents users from connecting to the server. `Warn But Allow` is the default value. ■ `Full Security`. If any type of certificate error occurs, users cannot connect to the server. Horizon Client displays certificate errors to the user. When this setting is configured, users can view the selected certificate verification mode in Horizon Client, but cannot configure the setting. The certificate checking mode dialog box informs users that an administrator has locked the setting. When this setting is disabled, Horizon Client users can select a certificate checking mode. This setting is disabled by default. To allow a server to perform selecting of certificates provided by Horizon Client, the client must make HTTPS connections to the Connection Server or security server host. Certificate checking is not supported if you off-load TLS to an intermediate device that makes HTTP connections to the Connection Server or security server host. If you do not want to configure this setting as a group policy, you can also enable certificate verification by adding the `CertCheckMode` value name to one of the following registry keys on the client computer: ■ For 64-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security` ■ For 64-bit Windows on ARM: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware VDM\Client\Security` Use the following values in the registry key: ■ **0** implements `No Security`. ■ **1** implements `Warn But Allow`. ■ **2** implements `Full Security`.

Table 3-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Computer	User	Description
			If you configure both the group policy setting and the `CertCheckMode` setting in the Windows Registry key, the group policy setting takes precedence over the registry key value. **Note** In a future Horizon Client release, using the Windows registry to configure this setting might not be supported and the group policy setting must be used.
`Default value of the 'Log in as current user' checkbox`	X	X	Specifies the default value of **Log in as current user** in the **Options** menu on the Horizon Client menu bar. This setting overrides the default value specified during Horizon Client installation. If a user runs Horizon Client from the command line and specifies the `logInAsCurrentUser` option, that value overrides this setting. When **Log in as current user** is selected in the **Options** menu, the identity and credential information that the user provided when logging in to the client system is passed to the Connection Server instance and ultimately to the remote desktop or published application. When **Log in as current user** is deselected, users must provide identity and credential information multiple times before they can access a remote desktop or published application. This setting is disabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser`.
`Display option to Log in as current user`	X	X	Determines whether **Log in as current user** is visible in the **Options** menu on the Horizon Client menu bar. When **Log in as current user** is visible, users can select or deselect it and override its default value. When **Log in as current user** is hidden, users cannot override its default value from the Horizon Client **Options** menu. You can specify the default value for **Log in as current user** by using the policy setting `Default value of the 'Log in as current user' checkbox`. This setting is enabled by default. The equivalent Windows Registry value is `LogInAsCurrentUser_Display`.
`Enable jump list integration`	X		Determines whether a jump list appears in the Horizon Client icon on the taskbar of Windows 7 and later systems. The jump list enables users to connect to recent servers, remote desktops, and published applications. If Horizon Client is shared, you might not want users to see the names of recent desktops and published applications. You can disable the jump list by disabling this setting. This setting is enabled by default. The equivalent Windows Registry value is `EnableJumplist`.

Table 3-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Computer	User	Description
`Enable SSL encrypted framework channel`	X	X	Determines whether TLS is enabled for View 5.0 and earlier remote desktops. Before View 5.0, the data sent over port TCP 32111 to the remote desktop was not encrypted. - **Enable**: Enables TLS, but allows fallback to the previous unencrypted connection if the remote desktop does not have TLS support. For example, View 5.0 and earlier remote desktops do not have TLS support. **Enable** is the default setting. - **Disable**: Disables TLS. This setting might be useful for debugging, or if the channel is not being tunneled and might potentially be optimized by a WAN accelerator product. - **Enforce**: Enables TLS and refuses to connect to remote desktops that do not have TLS support . The equivalent Windows Registry value is `EnableTicketSSLAuth`.
`Configure SSL protocols and cryptographic algorithms`	X	X	Enables you to specify cryptographic algorithms and protocols before establishing an encrypted SSL connection.. The cipher list consists of one or more cipher strings separated by colons. The cipher string is case-sensitive. If the feature is enabled, the default value is **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** This cipher string means that TLS v1.1 and TLS v1.2 are enabled. Cipher suites will use ECDHE, ECDH, and RSA with 128 or 256 bit AES, with a preference for GCM mode. SSL v2.0, SSL v3.0 and TLS v1.0 are not supported. For more information, see http://www.openssl.org/docs/apps/ciphers.html. The equivalent Windows Registry value is `SSLCipherList`. Configure signature algorithms specifics the signature algorithms for TLS v1.2. Enter a colon separated list of signature algorithms in order of decreasing preference, in the form of algorithm+hash. Note that algorithm and hash names are case sensitive. For example: **RSA+SHA256:ECDSA+SHA256**. If this option is not set, the default value is all signature algorithms supported by the OpenSSL library. The equivalent Windows Registry value for the Configure signature algorithms is **SSLSignatureAlgorithms**. Configure supported groups sets the supported elliptic curve groups. Enter a list of curves separated by colons. Note that curve names are case sensitive. For example: **P-256:P-384**. If this option is not set and ECDHE cipher suites are provided, then the default value is all signature algorithms supported by the OpenSSL library. The equivalent Windows Registry value for the Configure supported groups is **SSLSupportedGroups**.

Table 3-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Computer	User	Description
`Enable Single Sign-On for smart card authentication`	X		Determines whether single sign-on is enabled for smart card authentication. When single sign-on is enabled, Horizon Client stores the encrypted smart card PIN in temporary memory before submitting it to Connection Server. When single sign-on is disabled, Horizon Client does not display a custom PIN dialog box. The equivalent Windows Registry value is `EnableSmartCardSSO`.
`Ignore certificate revocation problems`	X	X	Determines whether to check certificate revocation status. When this GPO is enabled, the Horizon Client will treat the server's certificate as valid even if the certificate sent by the server has been revoked or certificate revocation checking is known to be impossible, for instance if internet connection is limited. This setting is disabled by default. **Note** When this setting is enabled, the client might only use a cached URL during server certificate verification. The types of cached URL information can be CRL Distribution Point (CDP) and Authority Information Access (OCSP and CA issuer access methods).
Protocol connection certificate verification mode			Determines the certificate check mode for blast and tunnel connections. ■ **Thumbprint Verification**: If certificate thumbprint verification fails, the connection to the virtual entitlement is blocked. ■ **Thumbprint or PKI Verification**: Certificate thumbprint errors fall back to PKI certificate verification, If the PKI certificate check fails, the connection to the virtual entitlement is blocked. ■ **PKI and Thumbprint Verification**: The client uses both PKI and Thumbprint verification. If either of these fails, the connection to the virtual entitlement is blocked. When this property is set to PKI Verification, and the PKI certificate authentication fails, the connection to the virtual entitlement is blocked. The default value is **Thumbprint Verification**. The equivalent Windows Registry value is **ProtocolConnectionCertCheckMode**.

Table 3-5. Horizon Client Configuration Template: Security Settings (continued)

Setting	Computer	User	Description
Strict certificate revocation check			When this GPO is enabled, the Horizon Client refuses to connect to servers when it cannot verify the certificate revocation status. When this setting is disabled, the client checks revocation but it will not block a connection based on revocation status. The **DoNotCheckCertRevocationStatus** GPO takes precedence over this GPO.This setting is disabled by default. The equivalent Windows Registry value is **StrictCertRevocationCheck**.
`Unlock remote sessions when the client machine is unlocked`	X	X	Determines whether the Recursive Unlock feature is enabled. The Recursive Unlock feature unlocks all remote sessions after the client machine has been unlocked. This feature applies only after a user logs in to the server with the Log in as current user feature. This setting is enabled by default.

The following settings appear in the **VMware Horizon Client Configuration > Security Settings > NTLM Settings** folder in the Group Policy Management Editor.

Table 3-6. Horizon Client Configuration Template: Security Settings, NTLM Authentication Settings

Setting	Computer	User	Description
`Allow NTLM Authentication`	X		When this setting is enabled, NTLM authentication is allowed with the **Log in as current user** feature. When this setting is disabled, NTLM authentication is not used for any servers. When this setting is enabled, you can select **Yes** or **No** from the **Allow fallback from Kerberos to NTLM** drop-down menu. ■ If you select **Yes**, NTLM authentication may be used any time that the client is unable to retrieve a Kerberos ticket for the server. ■ If you select **No**, NTLM authentication is allowed only for servers listed in the **Always use NTLM servers** group policy setting. When this setting is not configured, NTLM authentication is allowed for the servers listed in the **Always use NTLM servers** group policy setting. To use NTLM authentication, the server SSL certificate must be valid and Windows policies must not restrict the use of NTLM. For information about configuring fallback from Kerberos to NTLM in a Connection Server instance, see "Using the Log In as Current User Feature Available with Windows-Based Horizon Client" in the *VMware Horizon Console Administration* document.
`Always use NTLM for servers`	X		When this setting is enabled, the **Log in as current user** feature always uses NTLM authentication for the listed servers. To create the server list, click **Show** and enter the server name in the **Value** column. The naming format for servers is the fully qualified domain name (FQDN).

RDP Settings for Client GPOs

You can configure group policy settings for options such as the redirection of audio, printers, ports, and other devices when you use the Microsoft RDP display protocol.

The following table describes the Remote Desktop Protocol (RDP) settings in the Horizon Client Configuration ADMX template file. All RDP settings are User Configuration settings. The settings appear in the **VMware Horizon Client Configuration > RDP Settings** folder in the Group Policy Management Editor.

Table 3-7. Horizon Client Configuration Administrative Template: RDP Settings

Setting	Description
`Audio redirection`	Determines whether audio information played on the remote desktop is redirected. Select one of the following settings: - **Disable Audio**: Audio is disabled. - **Play in VM (needed for VoIP USB Support)**: Audio plays within the remote desktop. This setting requires a shared USB audio device to provide sound on the client. - **Redirect to client**: Audio is redirected to the client. This setting is the default mode. This setting applies only to RDP audio. Audio that is redirected through MMR plays in the client.
`Enable audio capture redirection`	Determines whether the default audio input device is redirected from the client to the remote session. When this setting is enabled, the audio recording device on the client appears in the remote desktop and can record audio input. The default setting is disabled.
`Bitmap cache file size in` *unit* `for` *number* `bpp bitmaps`	Specifies the size of the bitmap cache, in kilobytes or megabytes, to use for specific bits per pixel (bpp) bitmap color settings. Separate versions of this setting are provided for the following unit and bpp combinations: - MB/8bpp - MB/16bpp - MB/24bpp - MB/32bpp
`In-memory bitmap cache size in KB for 8bpp bitmaps`	Specifies the size, in kilobytes, of the RAM bitmap cache to use for the 8-bits-per-pixel color setting. If ScaleBitmapCachesByBPP is true (the default), this cache size is multiplied by the bytes per pixel to determine the actual RAM cache size. When this setting is enabled, enter a size in kilobytes.
`Bitmap caching/cache persistence active`	Determines whether persistent bitmap caching is used (active). Persistent bitmap caching can improve performance, but it requires additional disk space.
`Color depth`	Specifies the color depth of the remote desktop. Select one of the available settings: - 8 bit - 15 bit - 16 bit - 24 bit - 32 bit
`Cursor shadow`	Determines whether a shadow appears under the pointer on the remote desktop.
`Desktop background`	Determines whether the desktop background appears when clients connect to a remote desktop.
`Desktop composition`	Determines whether desktop composition is enabled on the remote desktop. When desktop composition is enabled, individual windows no longer draw directly to the screen or primary display device as they did in previous versions of Microsoft Windows. Instead, drawing is redirected to off-screen surfaces in video memory, which are then rendered into a desktop image and presented on the display.

Table 3-7. Horizon Client Configuration Administrative Template: RDP Settings (continued)

Setting	Description
`Enable compression`	Determines whether RDP data is compressed. This setting is enabled by default.
`Enable RDP Auto-Reconnect`	Determines whether the RDP client component attempts to reconnect to a remote desktop after an RDP protocol connection failure. This setting has no effect if the **Use secure tunnel connection to desktop** option is enabled in Horizon Console. This setting is disabled by default.
`Font smoothing`	Determines whether anti-aliasing is applied to the fonts on the remote desktop.
`Menu and window animation`	Determines whether animation for menus and windows is enabled when clients connect to a remote desktop.
`Redirect clipboard`	Determines whether the local clipboard information is redirected when clients connect to the remote desktop.
`Redirect drives`	Determines whether local disk drives are redirected when clients connect to the remote desktop. By default, local drives are redirected. Enabling this setting, or leaving it unconfigured, allows data on the redirected drive on the remote desktop to be copied to the drive on the client computer. Disable this setting if allowing data to pass from the remote desktop to users' client computers represents a potential security risk in your deployment. Another approach is to disable folder redirection in the remote desktop virtual machine by enabling the Microsoft Windows group policy setting, `Do not allow drive redirection`. The `Redirect drives` setting applies to RDP only.
`Redirect printers`	Determines whether local printers are redirected when clients connect to the remote desktop.
`Redirect serial ports`	Determines whether local COM ports are redirected when clients connect to the remote desktop.
`Redirect smart cards`	Determines whether local smart cards are redirected when clients connect to the remote desktop. **Note** This setting applies to both RDP and PCoIP connections.
`Redirect supported plug-and-play devices`	Determines whether local plug-and-play and point-of-sale devices are redirected when clients connect to the remote desktop. This behavior is different from the redirection that the USB Redirection component of the agent manages.
`Shadow bitmaps`	Determines whether bitmaps are shadowed. This setting has no effect in full-screen mode.
`Show contents of window while dragging`	Determines whether the folder contents appear when users drag a folder to a new location.
`Themes`	Determines whether themes appear when clients connect to a remote desktop.

Table 3-7. Horizon Client Configuration Administrative Template: RDP Settings (continued)

Setting	Description
`Windows key combination redirection`	Determines where Windows key combinations are applied. This setting lets you send key combinations to the remote virtual machine or apply key combinations locally. Key combinations are applied locally by default.
`Enable Credential Security Service Provider`	Specifies whether the remote desktop connection uses Network Level Authentication (NLA). If the guest operating system requires NLA for remote desktop connections, you must enable this setting or Horizon Client might not connect to the remote desktop. In addition to enabling this setting, you must also verify that the following conditions are met: ■ Both the client and guest operating systems support NLA. ■ Direct client connections are enabled for the Connection Server instance. Tunneled connections are not supported with NLA.

General Settings for Client GPOs

General settings include proxy options, time zone forwarding, multimedia acceleration, and other display settings.

The following table describes the general settings in the Horizon Client Configuration ADMX template file. General settings include both Computer Configuration and User Configuration settings. The User Configuration setting overrides the equivalent Computer Configuration setting. The settings appear in the **VMware Horizon Client Configuration** folder in the Group Policy Management Editor.

Table 3-8. Horizon Client Configuration Template: General Settings

Setting	Computer	User	Description
`Allow Blast connections to use operating system proxy settings`	X		Configures proxy server use for VMware Blast connections. When this setting enabled, VMware Blast can connect through a proxy server. When this setting is disabled, VMware Blast cannot use a proxy server. When this setting is not configured (the default), users can configure whether VMware Blast connections can use a proxy server in the Horizon Client user interface. See Configure VMware Blast Options.
`Allow data sharing`	X		When this setting is enabled, the data sharing mode setting in the Horizon Client user interface is set to On and end users cannot change the setting. When this setting is disabled, the data sharing mode setting in the Horizon Client user interface is set to Off and end users cannot change the setting. When this setting is not configured (the default), end users can change the data sharing mode setting in the Horizon Client user interface.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Allow display scaling`	X	X	When this setting is enabled, the display scaling feature is enabled for all remote desktops and published applications. When this setting is disabled, the display scaling feature is disabled for all remote desktops and published applications. If this setting is not configured (the default setting), end users can enable and disable display scaling in the Horizon Client user interface. You can also hide the display scaling preference in the Horizon Client user interface by enabling the **Locked Guest Size** group policy setting.
`Allow H.264 Decoding`	X		Configures H.264 decoding for the VMware Blast protocol. When this setting is enabled, H.264 decoding becomes the preferred option. When this setting is disabled, H.264 decoding is never used. When this setting is not configured, users can choose whether to enable H.264 decoding. See Configure VMware Blast Options.
`Allow H.264 high color accuracy`	X		Configures high-color accuracy mode for H.264. This setting takes effect only if H.264 decoding is enabled. When this setting is not configured, users can choose whether to enable high-color accuracy mode. See Configure VMware Blast Options.
`Allow HEVC Decoding`	X		Configures HEVC (also known as H.265) decoding for the VMware Blast protocol. When this setting is enabled, HEVC decoding becomes the preferred option. When this setting is disabled, HEVC decoding is never used. When this setting is not configured, users can choose whether to enable HEVC decoding. See Configure VMware Blast Options.
`Allow user to skip Horizon Client update`	X		Specifies whether users can click the **Skip** button in the Horizon Client update window. If users click **Skip**, they do not see another update notification until the next Horizon Client version is available.
`Always hide the remote floating language (IME) bar for Hosted Apps`	X	X	Forces the floating language bar off for application sessions. When this setting is enabled, the floating language bar is never shown in a published application session, regardless of whether the local IME feature is enabled. When this setting is disabled, the floating language bar is shown only if the local IME feature is disabled. This setting is disabled by default.
`Always on top`		X	Determines whether the Horizon Client window is always the topmost window. Enabling this setting prevents the Windows taskbar from obscuring a full-screen Horizon Client window. This setting is disabled by default.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Automatic input focus in a virtual desktop window`	X	X	When this setting is enabled, Horizon Client sends input to the remote desktop automatically when a user brings the remote desktop to the front. In other words, focus is not in the frame of the window, and the user does not need to click inside the remote desktop window to move focus.
`Automatically check for updates`	X		Specifies whether to check for Horizon Client software updates automatically. This setting controls the **Check for updates and show badge notification** check box on the Horizon Client update window. This setting is enabled by default.
`Automatically install shortcuts when configured on the Horizon server`	X	X	When published application and remote desktop shortcuts are configured on a Connection Server instance, this setting specifies how and whether the shortcuts are installed on client machines when users connect to the server. When this setting is enabled, shortcuts are installed on client machines. Users are not prompted to install the shortcuts. When this setting is disabled, shortcuts are never installed on client machines. Users are not prompted to install the shortcuts. Users are prompted to install the shortcuts by default.
`Automatically synchronize the keypad, scroll and caps lock keys`	X		When this setting is enabled, the toggle states of the Num Lock, Scroll Lock, and Caps Lock keys are synchronized from the client device to a remote desktop. In Horizon Client, the **Automatically synchronize the keypad, scroll and cap lock keys** setting check box is selected and the setting is dimmed. When this setting is disabled, the lock key toggle states are synchronized from the remote desktop to the client device. In Horizon Client, the **Automatically synchronize the keypad, scroll and cap lock keys** setting check box is deselected and the setting is dimmed. When this setting is either enabled or disabled, users cannot modify the **Automatically synchronize the keypad, scroll and cap lock keys** setting in Horizon Client. When this setting is not configured, a user can enable or disable lock key synchronization for a remote desktop by configuring the **Automatically synchronize the keypad, scroll and cap lock keys** setting in Horizon Client. See Configure Lock Key Synchronization. This setting is not configured by default.
`Block multiple Horizon Client instances per Windows session`	X		Prevents a user from starting multiple Horizon Client instances during a Windows session. When this setting is enabled, Horizon Client runs in single-instance mode and a user cannot start multiple Horizon Client instances in a Windows session. When this setting is disabled, a user can start multiple Horizon Client instances in a Windows session. This setting is disabled by default.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Configure maximum latency for mouse coalescing`	X		Sets the maximum latency allowed, in milliseconds, when coalescing mouse movement events. Valid values are 0 through 50. A value of 0 disables the feature. Coalescing mouse movement events can reduce client-to-agent bandwidth use, but can potentially add minor latency to mouse movement. This setting is disabled by default.
`Custom error screen footer`	X		Enables you to add custom help text to the bottom of all Horizon Client error messages. You must provide the help text in a plain text (`.txt`) file on the local client system. The text file can contain up to 2048 characters, including control characters. Both ANSI and Unicode encoding are supported. When this setting is enabled, you specify the full path to the file that contains the custom help text in the text box provided, for example, `C:\myDocs\errorFooter.txt`. This setting is disabled by default.
`Default value of the "Hide the selector after launching an item" check box`	X	X	Sets whether the **Hide the selector after launching an item** check box is selected by default. This setting is disabled by default.
`Disable desktop disconnect messages`	X	X	Specifies whether messages that are normally shown upon remote desktop disconnection are disabled. These messages are shown by default.
`Disable sharing files and folders`		X	Specifies whether client drive redirection functionality is available in Horizon Client. When this setting is enabled, all client drive redirection functionality is disabled in Horizon Client, including the ability to open local files with published applications. In addition, the following elements are hidden in the Horizon Client user interface: ■ Sharing panel in the Settings dialog box. ■ **Share Folders** item in the **Option** menu in a remote desktop. ■ **Sharing** item for Horizon Client in the system tray. ■ Sharing dialog box that appears the first time you connect to a remote desktop or application after you connect to a server. When this setting is disabled, the client drive redirection feature is fully functional. This setting is disabled by default.
`Disable time zone forwarding`	X		Determines whether time zone synchronization between the remote desktop and the connected client is disabled.
`Disable toast notifications`	X	X	Determines whether to disable toast notifications from Horizon Client. Enable this setting if you do not want the user to see toast notifications in the corner of the screen. **Note** If you enable this setting, the user does not see a five-minute warning when the Session Timeout function is active.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Disallow passing through client information in a nested session`	X		Specifies whether Horizon Client is prevented from passing through client information in a nested session. When enabled, if Horizon Client is running inside a remote session, it sends the actual physical client information instead of the virtual machine device information. This setting applies to the following client information: device name and domain, client type, IP address, and MAC address. This setting is disabled by default, which means passing through client information in a nested session is allowed.
`Display modifier function key`	X	X	Specifies the switch modifier and function key combination that a user can press that, when grabbed and injecting input into a PCoIP or VMware Blast remote desktop session, changes the display configuration on the client machine. When this setting is not configured (the default setting), the end user must use the mouse to ungrab the remote desktop and then press the Windows logo key + P to select a presentation display mode. This setting does not apply to published application sessions.
`Disable opening local files in hosted applications`		X	Specifies whether Horizon Client registers local handlers for the file extensions that hosted applications support. When this setting is enabled, Horizon Client does not register any file extension handlers and does not allow the user to override the setting. When this setting is disabled, Horizon Client always registers file extension handlers. By default, file extension handlers are registered, but users can disable the feature in the Horizon Client user interface by using the **Turn on the ability to open a local file with a remote application from the local file system** setting on the Sharing panel in the Settings dialog box. For more information, see Share Local Folders and Drives. This setting is disabled by default.
`Display only smart card certificates during login`	X		Specifies whether to list all certificates from user and system stores or to show only certificates of smart cards. When this setting is enabled, the certificate selection dialog box displays only smart card certificate. When this setting is disabled, all certificate displayed. This setting is disabled by default.
`Don't check monitor alignment on spanning`		X	By default, the client desktop does not span multiple monitors if the screens do not form an exact rectangle when they are combined. Enable this setting to override the default. This setting is disabled by default.
`Enable Horizon Client Window Optimizations`	X	X	Reduces CPU usage when the Horizon Client window is not fully visible. This setting is enabled by default.
`Enable multi-media acceleration`		X	Determines whether multimedia redirection (MMR) is enabled on the client. MMR does not work correctly if the Horizon Client video display hardware does not have overlay support.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Enable relative mouse`	X	X	Enables the relative mouse when using the PCoIP display protocol. Relative mouse mode improves the mouse behavior for certain graphics applications and games. If the remote desktop does not support the relative mouse, this setting is not used. This setting is disabled by default.
`Enable the shade`		X	Determines whether the shade menu bar at the top of the Horizon Client window is visible. This setting is enabled by default. **Note** The shade menu bar is disabled by default for kiosk mode.
`Enable Horizon Client online update`	X		Enables the online update feature. This setting is enabled by default. **Note** You can also disable the online update feature by setting the `AUTO_UPDATE_ENABLED` property to 0 when you install Horizon Client from the command line. For more information, see Install Horizon Client From the Command Line.
`Enable Split Mks Window`	X		This setting provides a temporary workaround for multi-monitor display problems encountered when using Horizon Client for Windows 2106 or later with unified communications (UC) applications such as Cisco WebEx and Zoom. This setting is enabled by default. If your UC vendor has not yet provided an application update that fixes the display problem, you can implement a temporary workaround by disabling this setting. Disabling this setting turns off the default windows hierarchy and causes windows to be displayed in relation to the bounding box of all monitors in a multi-monitor setup. For more information, see VMware Knowledge Base (KB) article 85400. **Note** Use this workaround only as a temporary fix until you can install the updated version of the UC application that fixes the display problem permanently. After installing the updated UC application, turn on the default windows hierarchy again by enabling this setting from the GPO.
`Hide items in application context menu`	X	X	Use this setting to hide items in the context menu that appears when you right-click a published application in the desktop and application selector window. When this setting is enabled, you can configure the following options: ■ **Hide Settings** -- Select **Yes** to hide the **Settings** item in the context menu. ■ **Hide Create Shortcut to Desktop** -- Select **Yes** to hide the **Create Shortcut to Desktop** item in the context menu. ■ **Hide Add to Start Menu** -- Select **Yes** to hide the **Add to Start Menu** item in the context menu. ■ **Hide Mark as Favorite** -- Select **Yes** to hide the **Mark as Favorite** item in the context menu. This setting is disabled by default.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Hide items in desktop context menu`	X	X	Use this setting to hide items in the context menu that appears when you right-click a remote desktop in the desktop and application selector window. When this setting is enabled, you can configure the following options: ■ **Hide Reset Desktop** -- Select **Yes** to hide the **Reset Desktop** item in the context menu. ■ **Hide Restart Desktop** -- Select **Yes** to hide the **Restart Desktop** item in the context menu. ■ **Hide Display** -- Select **Yes** to hide the **Display** item in the context menu. ■ **Hide Settings** -- Select **Yes** to hide the **Settings** item in the context menu. ■ **Hide Create Shortcut to Desktop** -- Select **Yes** to hide the **Create Shortcut to Desktop** item in the context menu. ■ **Hide Add to Start Menu** -- Select **Yes** to hide the **Add to Start Menu** item in the context menu. ■ **Hide Mark as Favorite** -- Select **Yes** to hide the **Mark as Favorite** item in the context menu. This setting is disabled by default.
`Hide items in desktop toolbar`	X	X	Use this setting to hide items on the menu bar in a remote desktop window. When this setting is enabled, you can configure the following options. ■ **Hide Help** -- Select **Yes** to hide the **Help** item in the **Options** menu. ■ **Hide Reset Desktop** -- Select **Yes** to hide the **Reset Desktop** item from the **Options** menu. ■ **Hide Restart Desktop** -- Select **Yes** to hide the **Restart Desktop** item from the **Options** menu. ■ **Hide Connect USB Device** -- Select **Yes** to hide the **Connect USB Device** menu on the menu bar. This setting is disabled by default.
`Hide items in system tray menu`	X	X	Use this setting to hide items in the context menu that appears when you right-click the Horizon Client icon in the system tray on the local client system. When this setting is enabled, you can configure the following options. ■ **Hide Settings** -- Select **Yes** to hide the Horizon Client **Settings** item. This setting is disabled by default.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Hide items in the client toolbar menu`	X	X	Use this setting to hide items in the toolbar at the top of the desktop and application selector window. When this setting is enabled, you can configure the following options. ■ **Hide Favorites Toggle** -- Select **Yes** to hide the **Show Favorites** (star) icon. ■ **Hide Settings Gear** -- Select **Yes** to hide the **Settings** (gear) icon. This setting is disabled by default.
`Hotkey combination to grab input focus`	X	X	Configures a hot key combination to grab input focus for the last-used PCoIP or VMware Blast remote desktop session. The hot key consists of one or two modifier keys and one letter key. When this setting is disabled or not configured, the user can grab focus by clicking inside the remote desktop window. This setting is not configured by default.
`Hotkey combination to release input focus`	X	X	Configures a hot key combination to release input focus from a PCoIP or VMware Blast remote desktop session. The hot key consists of one or two modifier keys and one function key. When the **Minimize the fullscreen virtual desktop after release input focus** check box is selected, users can press any hot key that is configured to release input focus (for example, Ctrl+Shift+F5) to minimize the remote desktop window when the remote desktop is in full-screen mode. By default, Ctrl+Shift+F5 minimizes the remote desktop window when the desktop is in full-screen mode without any configuration. When this setting is disabled or not configured, the user can release focus by pressing Ctrl+Alt or clicking outside the remote desktop window. This setting is not configured by default.
`Pin the shade`		X	Determines whether the pin on the shade at the top of the Horizon Client window is enabled and auto-hiding of the menu bar does not occur. This setting has no effect if the shade is disabled. This setting is enabled by default.
`Save resolution and DPI to server`	X		Determines whether Horizon Client saves custom display resolution and display scaling settings on the server. For information about customizing the display resolution and display scaling settings for a remote desktop, see Customize the Display Resolution and Display Scaling for a Remote Desktop. When this setting is enabled, and the display resolution or display scaling has been customized for a remote desktop, each time a user opens the remote desktop, the custom settings are applied automatically, regardless of the client device that the user uses to log in to the remote desktop. This setting is disabled by default.
`Tunnel proxy bypass address list`	X		Specifies a list of tunnel addresses. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries.

Table 3-8. Horizon Client Configuration Template: General Settings (continued)

Setting	Computer	User	Description
`Update message pop-up`	X		Specifies whether to show the update pop-up message to end users automatically when a new version of Horizon Client is available. This setting controls the **Show pop-up message when there is an update** check box on the Horizon Client update window. This setting is disabled by default.
`URL for Horizon Client online help`	X		Specifies an alternate URL from which Horizon Client can retrieve help pages. This setting is intended for use in environments that cannot retrieve the remotely hosted help system because they do not have Internet access.
`URL for Horizon Client online update`	X		Specifies an alternate URL from which Horizon Client can retrieve updates. This setting is intended for use in an environment that defines its own private/personal update center. If it is not enabled, the VMware official update server is used.

USB Settings for Client GPOs

You can define USB policy settings for Horizon Agent and Horizon Client. On connection, Horizon Client downloads the USB policy settings from Horizon Agent and uses those settings, together with the Horizon Client USB policy settings, to determine which devices are available for redirection from the host machine.

The following table describes each policy setting for splitting composite USB devices in the Horizon Client Configuration ADMX template file. The settings apply at the computer level. The settings from the GPO at the computer level take precedence over the registry at `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB`. The settings appear in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

For more information about using policies to control USB redirection, see the *Configuring Remote Desktop Features in Horizon* document.

Table 3-9. Horizon Client Configuration Template: USB Splitting Settings

Setting	Description
Allow Auto Device Splitting	Allow the automatic splitting of composite USB devices. The default value is undefined, which equates to **false**.
Exclude Vid/Pid Device From Split	Excludes a composite USB device specified by vendor and product IDs from splitting. The format of the setting is vid-*xxx1*_pid-*yyy2*[;vid-*xxx2*_pid-*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (*) in place of individual digits in an ID. For example: **vid-0781_pid-55**** The default value is undefined.
Split Vid/Pid Device	Treats the components of a composite USB device specified by vendor and product IDs as separate devices. The format of the setting is vid-*xxxx*_pid-*yyyy*(exintf:*zz*[;exintf:*ww*]) You can use the exintf keyword to exclude components from redirection by specifying their interface number. You must specify ID numbers in hexadecimal, and interface numbers in decimal including any leading zero. You can use the wildcard character (*) in place of individual digits in an ID. For example: **vid-0781_pid-554c(exintf:01;exintf:02)** **Note** Horizon does not automatically include the components that you have not explicitly excluded. You must specify a filter policy such as Include Vid/Pid Device to include those components. The default value is undefined.

The following table describes the policy settings in the Horizon Client Configuration ADMX template file for filtering USB devices. The settings apply at the computer level. The settings from the GPO at the computer level take precedence over the registry at HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\USB.

For more information about configuring filter policy settings for USB redirection, see the *Configuring Remote Desktop Features in Horizon* document.

Table 3-10. Horizon Client Configuration Template: USB Filtering Settings

Setting	Description
Allow Audio Input Devices	Allows audio input devices to be redirected. The default value is undefined, which equates to **true**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
Allow Audio Output Devices	Allows audio output devices to be redirected. The default value is undefined, which equates to **false**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

Table 3-10. Horizon Client Configuration Template: USB Filtering Settings (continued)

Setting	Description
`Allow HID-Bootable`	Allows input devices other than keyboards or mice that are available at startup time (also known as hid-bootable devices) to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Device Descriptor Failsafe Behavior`	Allows devices to be redirected even if the Horizon Client fails to get the config/device descriptors. To allow a device even if it fails the config/desc, include it in the Include filters, such `IncludeVidPid` or `IncludePath`. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Allow Other Input Devices`	Allows input devices other than hid-bootable devices or keyboards with integrated pointing devices to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Keyboard and Mouse Devices`	Allows keyboards with integrated pointing devices (such as a mouse, trackball, or touch pad) to be redirected. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Smart Cards`	Allows smart-card devices to be redirected. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Allow Video Devices`	Allows video devices to be redirected. The default value is undefined, which equates to **`true`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Disable Remote Configuration`	Disables the use of agent settings when performing USB device filtering. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.

Table 3-10. Horizon Client Configuration Template: USB Filtering Settings (continued)

Setting	Description
`Exclude All Devices`	Excludes all USB devices from being redirected. If set to **`true`**, you can use other policy settings to allow specific devices or families of devices to be redirected. If set to **`false`**, you can use other policy settings to prevent specific devices or families of devices from being redirected. If you set the value of `Exclude All Devices` to **`true`** on the agent, and this setting is passed to Horizon Client, the agent setting overrides the Horizon Client setting. The default value is undefined, which equates to **`false`**. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

`Exclude Automatically Connection Device Family`	Excludes families of devices from being forwarded automatically. Use the following syntax:
	`family-name[;...]`
	For example:
	`storage;hid`

`Exclude Automatically Connection Vid/Pid Device`	Excludes devices that have specific vendor and product IDs from being forwarded automatically. Use the following syntax:
	`vid-xxxx_pid-xxxx|*[;...]`
	For example:
	`vid-0781_pid-554c;vid-0781_pid-9999`

`Exclude Device Family`	Excludes families of devices from being redirected. The format of the setting is *family_name_1*[;*family_name_2*]... For example: **`bluetooth;smart-card`** If you have enabled automatic device splitting, Horizon examines the device family of each interface of a composite USB device to decide which interfaces are excluded. If you have disabled automatic device splitting, Horizon examines the device family of the whole composite USB device. The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Exclude Vid/Pid Device`	Excludes devices that have specific vendor and product IDs from being redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (`*`) in place of individual digits in an ID. For example: **`vid-0781_pid-****;vid-0561_pid-554c`** The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

Table 3-10. Horizon Client Configuration Template: USB Filtering Settings (continued)

Setting	Description
`Exclude Path`	Exclude devices at specified hub or port paths from being redirected. The format of the setting is `bus-`*x1*[`/`*y1*]...`/port-`*z1*[`;bus-`*x2*[`/`*y2*]...`/port-`*z2*]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2/3_port-02;bus-1/1/1/4_port-ff`** The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Include Device Family`	Includes families of devices that can be redirected. The format of the setting is *family_name_1*[`;`*family_name_2*]... For example: **`storage`** The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.
`Include Path`	Include devices at a specified hub or port paths that can be redirected. The format of the setting is `bus-`*x1*[`/`*y1*]...`/port-`*z1*[`;bus-`*x2*[`/`*y2*]...`/port-`*z2*]... You must specify bus and port numbers in hexadecimal. You cannot use the wildcard character in paths. For example: **`bus-1/2_port-02;bus-1/7/1/4_port-0f`** The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration > Settings not configurable by Agent** folder in the Group Policy Management Editor.
`Include Vid/Pid Device`	Specifies USB devices that have a specified vendor and product ID that can be redirected. The format of the setting is `vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]... You must specify ID numbers in hexadecimal. You can use the wildcard character (**`*`**) in place of individual digits in an ID. For example: **`vid-0561_pid-554c`** The default value is undefined. This setting appears in the **VMware Horizon Client Configuration > View USB Configuration** folder in the Group Policy Management Editor.

In a nested mode or double-hop scenario, a user connects from the physical client system to a remote desktop, starts Horizon Client inside the remote desktop (the nested session), and connects to another remote desktop. To make the device work as expected in the nested session, you must configure the USB policy settings in the same way on both the physical client machine and in the nested session.

VMware Browser Redirection Settings for Client GPOs

You can configure group policy settings for the Browser Redirection feature.

The following table describes the Browser Redirection settings in the Horizon Client Configuration ADMX template file. All Browser Redirection settings are Computer Configuration settings. The settings appear in the **VMware Horizon Client Configuration > VMware Browser Redirection** folder in the Group Policy Management Editor.

For information about agent-side Browser Redirection settings, see the *Configuring Remote Desktop Features in Horizon* document.

Table 3-11. Horizon Client Configuration Template: VMware Browser Redirection Settings

Setting	Description
`Enable WebRTC camera and microphone access for browser redirection`	When this setting is enabled, redirected pages that use WebRTC have access to the client system's camera and microphone. This setting is enabled by default.
`Ignore certificate errors for browser redirection`	When this setting is enabled, certificate errors that occur in the redirected page are ignored and browsing proceeds. This setting is disabled by default.
`Enable cache for browser redirection`	When this setting is enabled, the browsing history, including cookies, is stored on the client system. **Note** Disabling this setting does not clear the cache. If you disable and then re-enable this setting, the cache is reused. This setting is enabled by default.

VMware Integrated Printing Settings for Client GPOs

You can configure group policy settings for the VMware Integrated Printing feature.

The following table describes the VMware Integrated Printing settings in the Horizon Client Configuration ADMX template file. The table shows whether the settings include both Computer Configuration and User Configuration settings, or only Computer Configuration settings. For the settings that include both types of settings, the User Configuration setting overrides the equivalent Computer Configuration setting. The settings appear in the **VMware Horizon Client Configuration > VMware Integrated Printing** folder in the Group Policy Management Editor.

For information about agent-side VMware Integrated Printing settings, see the *Configuring Remote Desktop Features in Horizon* document.

Table 3-12. Horizon Client Configuration Template: VMware Integrated Printing Settings

Setting	Computer	User	Description
`Do not redirect client printer(s)`	X	X	Determines whether client printers are redirected. When this setting is enabled, no client printers are redirected. When this setting is disabled or not configured, all client printers are redirected. This setting is not configured by default.
`Allow to redirect L1 local printers to inner session`	X	X	Determines whether to redirect L1 local printers to the inner session. VMware supports running Horizon Client inside a remote desktop. This configuration, commonly called nested mode, involves three layers and two hops, as follows: ■ L0 (endpoint) - physical machine where Horizon Client is installed. ■ L1 (first-hop remote desktop) - the remote desktop where both Horizon Client and Horizon Agent are installed. ■ L2 (second-hop published desktop or published application) - the published desktop or published application to which the second-hop client connects. When this setting is enabled, the L1 local printers are redirected to the inner session. When this setting is not configured or disabled, the L1 local printers are not redirected to the inner session. This setting is not configured by default.

PCoIP Client Session Variables ADMX Template Settings

The PCoIP Client Session Variables ADMX template file (`pcoip.client.admx`) contains policy settings related to the PCoIP display protocol. You can configure computer default values that an administrator can override, or you can configure user settings that an administrator cannot override. The settings that can be overridden appear in the **PCoIP Client Session Variables > Overridable Administrator Defaults** folder in the Group Policy Management Editor. The settings that cannot be overridden appear in the **PCoIP Client Session Variables > Not Overridable Settings** folder in the Group Policy Management Editor.

The ADMX files are available in `VMware-Horizon-Extras-Bundle-`*`YYMM-x.x.x-yyyyyyyy`*`.zip`, which you can download from the VMware Downloads site at https://my.vmware.com/web/vmware/downloads. Under Desktop & End-User Computing, select the VMware Horizon download, which includes the GPO Bundle containing the ZIP file.

Table 3-13. PCoIP Client Session Variables

Setting	Description
`Configure PCoIP client image cache size policy`	Controls the size of the PCoIP client image cache. The client uses image caching to store portions of the display that were previously transmitted. Image caching reduces the amount of data that is retransmitted. When this setting is disabled, PCoIP uses a default client image cache size of 250 MB. When you enable this setting, you can configure a client image cache size from a minimum of 50 MB to a maximum of 300 MB. The default value is 250 MB. This setting is disabled by default.
`Configure PCoIP event log cleanup by size in MB`	Enables the configuration of the PCoIP event log cleanup by size in MB. When this setting is configured, it controls the log file cleanup by size in MB. For example, for a non-zero setting of *m*, log files larger than *m* MB are silently deleted. A setting of 0 indicates no file cleanup by size. When this setting is disabled, the default event log cleanup by size in MB setting is 100. This setting is disabled by default.
`Configure PCoIP event log cleanup by time in days`	Enables the configuration of the PCoIP event log cleanup by time in days. When this setting is configured, it controls the log file cleanup by time in days. For example, for a non-zero setting of *n*, log files older than *n* days are silently deleted. A setting of 0 indicates no file cleanup by time. When this policy is disabled, the default event log cleanup by time in days setting is 7. This setting is disabled by default. The log file cleanup is performed once, when the session starts. Any change to the setting is not applied until the next session.
`Configure PCoIP event log verbosity`	Sets the PCoIP event log verbosity. The values range from 0 (least verbose) to 3 (most verbose). When this setting is enabled, you can set the verbosity level from 0 to 3. When the setting is disabled, the default event log verbosity level is 2. This setting is disabled by default. When this setting is modified during an active PCoIP session, the new setting takes effect immediately.
`Configure PCoIP session encryption algorithms`	Controls the encryption algorithms advertised by the PCoIP endpoint during session negotiation. Selecting one of the check boxes disables the associated encryption algorithm. You must enable at least one algorithm. This setting applies to both agent and client. The endpoints negotiate the actual session encryption algorithm that is used. If FIPS140-2 approved mode is enabled, the **Disable AES-128-GCM encryption** value is overridden if both AES-128-GCM encryption and AES-256-GCM encryption are disabled. If the `Configure SSL Connections` setting is disabled, both the Salsa20-256round12 and AES-128-GCM algorithms are available for negotiation by this endpoint. This setting is disabled by default. Supported encryption algorithms, in order of preference, are SALSA20/12-256, AES-GCM-128, and AES-GCM-256. By default, all supported encryption algorithms are available for negotiation by this endpoint.

Table 3-13. PCoIP Client Session Variables (continued)

Setting	Description
`Configure PCoIP virtual channels`	Specifies the virtual channels that can and cannot operate over PCoIP sessions. This setting also determines whether to disable clipboard processing on the PCoIP host. Virtual channels that are used in PCoIP sessions must appear on the virtual channel authorization list. Virtual channels that appear in the unauthorized virtual channel list cannot be used in PCoIP sessions. You can specify a maximum of 15 virtual channels for use in PCoIP sessions. Separate multiple channel names with the vertical bar (|) character. For example, the virtual channel authorization string to allow the mksvchan and vdp_rdpvcbridge virtual channels is **`mksvchan|vdp_rdpvcbridge`**. If a channel name contains the vertical bar or backslash (\) character, insert a backslash character before it. For example, type the channel name awk|ward\channel as **`awk\\|ward\\channel`**. When the authorized virtual channel list is empty, all virtual channels are disallowed. When the unauthorized virtual channel list is empty, all virtual channels are allowed. The virtual channels setting applies to both agent and client. Virtual channels must be enabled on both agent and client for virtual channels to be used. The virtual channels setting provides a separate check box that allows you to disable remote clipboard processing on the PCoIP host. This value applies to the agent only. By default, all virtual channels are enabled, including clipboard processing.
`Configure SSL cipher list`	Configures a TLS/SSL cipher list to restrict the use of cipher suites before establishing an encrypted TLS/SSL connection. The list consists of one or more cipher suite strings separated by colons. All cipher suite strings are case insensitive. The default value is ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. If this setting is configured, the **Enforce AES-256 or stronger ciphers for SSL connection negotiation** check box in the `Configure SSL connections to satisfy Security Tools` setting is ignored. This setting must be applied to both the PCoIP server and the PCoIP client.
`Configure SSL connections to satisfy Security Tools`	Specifies how TLS session negotiation connections are established. To satisfy security tools, such as port scanners, enable this setting and do the following: 1 Store the certificate for the Certificate Authority that signed any Server certificate to be used with PCoIP in the Trusted Root certificate store. 2 Configure the agent to load certificates only from the Certificate Store. If the Personal store for the Local Machine is used, leave the CA Certificate store name unchanged with the value ROOT, unless a different store location was used in step 1. If this setting is disabled, the AES-128 cipher suite is not available and the endpoint uses Certification Authority certificates from the machine account's MY store and Certification Authority certificates from the ROOT store. This setting is disabled by default.
`Configure SSL protocols`	Configures the OpenSSL protocol to restrict the use of certain protocols before establishing an encrypted TLS connection. The protocol list consists of one or more OpenSSL protocol strings separated by colons. All cipher strings are case insensitive. The default value is `TLS1.1:TLS1.2`, which means that TLS v1.1 and TLS v1.2 are enabled and SSL v2.0, SSLv3.0, and TLS v1.0 are disabled. If this setting is set in both the client and the agent, the OpenSSL protocol negotiation rule is followed.

Table 3-13. PCoIP Client Session Variables (continued)

Setting	Description
`Configure the Client PCoIP UDP port`	Specifies the UDP client port that is used by software PCoIP clients. The UDP port value specifies the base UDP port to use. If the base port is not available, the UDP port range value determines how many additional ports to try. The range spans from the base port to the sum of the base port and port range. For example, if the base port is 50002 and the port range is 64, the range spans from 50002 to 50066. This setting applies to the client only. By default, the base port is 50002 and the port range is 64.
`Configure the maximum PCoIP session bandwidth`	Specifies the maximum bandwidth, in kilobits per second, in a PCoIP session. The bandwidth includes all imaging, audio, virtual channel, USB, and control PCoIP traffic. Set this value to the overall capacity of the link to which your endpoint is connected, considering the number of expected concurrent PCoIP sessions. For example, with a single-user VDI configuration (a single PCoIP session) that connects through a 4Mbit/s Internet connection, set this value to 4Mbit, or 10% less than this value to leave some allowance for other network traffic. When you expect multiple concurrent PCoIP sessions to share a link, comprising either multiple VDI users or an RDS configuration, you might want to adjust the setting accordingly. However, lowering this value will restrict the maximum bandwidth for each active session. Setting this value prevents the agent from attempting to transmit at a higher rate than the link capacity, which would cause excessive packet loss and a poorer user experience. This value is symmetric. It forces the client and agent to use the lower of the two values that are set on the client and agent side. For example, setting a 4 Mbit/s maximum bandwidth forces the agent to transmit at a lower rate, even though the setting is configured on the client. When this setting is disabled on an endpoint, the endpoint imposes no bandwidth constraints. When this setting is enabled, the setting is used as the endpoint's maximum bandwidth constraint in kilobits per second. The default value is 900000 kilobits per second. This setting applies to the agent and the client. If the two endpoints have different settings, the lower value is used.
`Configure the PCoIP session bandwidth floor`	Specifies a lower limit, in kilobits per second, for the bandwidth that the PCoIP session reserves. This setting configures the minimum expected bandwidth transmission rate for the endpoint. When you use this setting to reserve bandwidth for an endpoint, the user does not have to wait for bandwidth to become available, which improves session responsiveness. Make sure that you do not over-subscribe the total reserved bandwidth for all endpoints. Make sure that the sum of bandwidth floors for all connections in your configuration does not exceed the network capability. The default value is 0, which means that no minimum bandwidth is reserved. When this setting is disabled, no minimum bandwidth is reserved. This setting is disabled by default. This setting applies to the agent and the client, but the setting only affects the endpoint on which it is configured. When this setting is modified during an active PCoIP session, the change takes effect immediately.

Table 3-13. PCoIP Client Session Variables (continued)

Setting	Description
`Configure the PCoIP session MTU`	Specifies the Maximum Transmission Unit (MTU) size for UDP packets for a PCoIP session. The MTU size includes IP and UDP packet headers. TCP uses the standard MTU discovery mechanism to set MTU and this setting does not affect it. The maximum MTU size is 1500 bytes. The minimum MTU size is 500 bytes. The default value is 1300 bytes. Typically, you do not have to change the MTU size. Change this value if you have an unusual network setup that causes PCoIP packet fragmentation. This setting applies to the agent and the client. If the two endpoints have different MTU size settings, the lowest size is used. If this setting is disabled or not configured, the client uses the default value in the negotiation with the agent.
`Configure the PCoIP transport header`	Configures the PCoIP transport header and sets the transport session priority. The PCoIP transport header is a 32-bit header that is added to all PCoIP UDP packets (only if the transport header is enabled and both side support it). The PCoIP transport header allows network devices to make better prioritization/QoS decisions when dealing with network congestion. The transport header is enabled by default. The transport session priority determines the PCoIP session priority reported in the PCoIP transport header. Network devices make better prioritization/QoS decisions based on the specified transport session priority. When the `Configure the PCoIP transport header` setting is enabled, the following transport session priorities are available: ■ **High** ■ **Medium** (default value) ■ **Low** ■ **Undefined** The PCoIP agent and client negotiate the transport session priority value. If the PCoIP agent specifies a transport session priority value, the session uses the agent-specified session priority. If only the client has specified a transport session priority, the session uses the client-specified session priority. If neither agent nor client has specified a transport session priority, or **Undefined Priority** is specified, the session uses the default value, **Medium** priority.
`Enable/disable audio in the PCoIP session`	Determines whether audio is enabled in PCoIP sessions. Both endpoints must have audio enabled. When this setting is enabled, PCoIP audio is allowed. When it is disabled, PCoIP audio is disabled. Audio is enabled by default.

Running Horizon Client From the Command Line

You can run Horizon Client from the command line or from scripts. You might want to run Horizon Client from the command line if you are implementing a kiosk-based application that grants end users access to remote desktop applications.

To run Horizon Client from the command line, you use the `vmware-view.exe` command. The `vmware-view.exe` command includes options that you can specify to change the behavior of Horizon Client.

Horizon Client Command Use

The syntax of the `vmware-view` command controls the operation of Horizon Client.

Use the following form of the `vmware-view` command from a Windows command prompt.

```
vmware-view [command_line_option [argument]] ...
```

The default path to the `vmware-view` command executable file depends on the client system. You can add this path to the *PATH* environment variable on the client system.

- 64-bit systems: `C:\Program Files\VMware\VMware Horizon View Client\`
- 64-bit systems on ARM: `C:\Program Files (x86)\VMware\VMware Horizon View Client\`

The following table shows the command-line options that you can use with the `vmware-view` command.

Table 3-14. Horizon Client Command-Line Options

Option	Description
`/?`	Displays the list of command options.
`-appName` *application_ name*	Specifies the name of the published application as it appears in the desktop and application selection window. The name is the display name that was specified for the application pool in the pool creation wizard.
`-appProtocol` *protocol*	Specifies the published application display protocol to use, if available. The valid protocols are as follows: ■ **Blast** ■ **PCoIP**
`-appSessionReconnectionBehavior` *argument*	Specifies the published application reconnection behavior setting. The valid arguments are as follows: **always** Implements the **Reconnect automatically to open applications** setting. **never** Implements the **Do not ask to reconnect and do not automatically reconnect** setting. **ask** Implements **Ask to reconnect to open applications** setting. When you use this option, the published application reconnection settings are disabled in Horizon Client.

`-args` *argument*	Specifies command-line arguments to add when a published application starts. For example:
	`vmware-view.exe -serverURL`
	`10.10.10.10 -appName "My Notepad++" -args "\"my new.txt\""`

Table 3-14. Horizon Client Command-Line Options (continued)

Option	Description
`-connectUSBOnStartup`	When set to `true`, redirects all USB devices that are connected to the host to the remote desktop or published application. This option is implicitly set if you specify the `-unattended` option for a remote desktop. The default is `false`.
`-connectUSBOnInsert`	When set to `true`, connects a USB device to the foreground remote desktop or published application when you plug in the device. This option is implicitly set if you specify the `-unattended` option for a remote desktop. The default is `false`.
`-desktopLayout` *window_size*	Specifies how to display the remote desktop window. The valid window size values are as follows: **`fullscreen`** Full-screen display. **`multimonitor`** Multiple-monitor display. **`windowLarge`** Large window. **`windowSmall`** Small window. **`length X width`** Custom size, for example, 800 X 600.
`-desktopName` *desktop_name*	Specifies the name of the remote desktop as it appears in the desktop and application selection window. The name is the display name that was specified for the pool in the pool creation wizard. **Important** Do not specify this option for clients in kiosk mode. This option has no effect when in the remote desktop runs in kiosk mode. For kiosk mode, the connection is made to the first remote desktop in the list of entitled remote desktops.
`-desktopProtocol` *protocol*	Specifies the display protocol to use as it appears in the desktop and application selection window. The valid display protocols are as follows: ■ **`Blast`** ■ **`PCoIP`** ■ **`RDP`**
`-domainName` *domain_name*	Specifies the NETBIOS domain that the end user uses to log in to Horizon Client. For example, use `mycompany` rather than `mycompany.com`.
`-file` *file_path*	Specifies the path of a configuration file that contains additional command options and arguments.
`-h`	Shows help options.
`-hideClientAfterLaunchSession`	When set to `true`, hides the desktop and application selector window. When set to `false`, shows the desktop and application selector window.

Table 3-14. Horizon Client Command-Line Options (continued)

Option	Description

`-installShortcutsThenQuit`	Use this option to install desktop and application shortcuts that are configured on the server. When you use this option with sufficient server authentication information, Horizon Client silently connects to the server, installs the shortcuts, and then quits. If server authentication fails, Horizon Client quits silently.
	To install shortcuts on the client system automatically, create a script that runs when the client system starts up. For example:
	`vmware-view.exe -serverURL serverurl -userName user`
	`-domainName domain`
	`-password password -installShortcutsThenQuit`
	
	`vmware-view.exe -serverURL serverurl -loginAsCurrentUser`
	`true -installShortcutsThenQuit`
	For information about server-created shortcuts, see Configure Start Menu Shortcut Updates.

`-languageId` *Locale_ID*	Provides localization support for different languages in Horizon Client. If a resource library is available, specify the Locale ID (LCID) to use. For US English, enter the value 0x409.
`-launchMinimized`	Starts Horizon Client in minimized mode. If you provide the `-appName` or `-desktopName` option, Horizon Client remains minimized until the specified published application or remote desktop starts. You cannot use this option with the `-unattended` or `-nonInteractive` option.

`-listMonitors`	Lists index values and display layout information for the connected monitors. For example:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (-900, -410, 0, 1190)`
	You use these index values in the `-monitors` option.

`-loginAsCurrentUser`	When set to `true`, uses the credential information that the end user provides when logging in to the client system to log in to the server and ultimately to the remote desktop. The default is `false`.
`-monitors "`*n*`[,`*n*`,`*n*`,`*n*`]"`	Specifies monitors to use in a multiple-monitor setup, where *n* is the index value of a monitor. You can use the `-listMonitors` option to determine the index values of the connected monitors. You can specify up to four index values, separated by commas. For example: `-monitors "1,2"` This option has no effect unless `-desktopLayout` is set to `multimonitor`.
`-nonInteractive`	Suppresses error message boxes when starting Horizon Client from a script. This option is implicitly set if you specify the `-unattended` option. **Note** If you log in to a server in non-interactive mode, you are not prompted to install **Start** menu shortcuts (if available), and shortcuts are installed by default.

Table 3-14. Horizon Client Command-Line Options (continued)

Option	Description
`-noVMwareAddins`	Prevents loading of VMware-specific virtual channels, such as Virtual Printing.
`-password` *password*	Specifies the password that the end user uses to log in to Horizon Client. The password is processed in plain text by the command console or any scripting tool. If you generate the password automatically, you do not need to specify this option for clients in kiosk mode. For improved security, do not specify this option. Users can enter the password interactively.
`-printEnvironmentInfo`	Displays the IP address, MAC address, and machine name of the client device.
`-serverURL` *connection_server*	Specifies the URL, IP address, or FQDN of the server.
`-shutdown`	Shuts down all remote desktops and published applications and relevant user interface components.
`-singleAutoConnect`	If the user is entitled to only one remote desktop or published application, connects to that remote desktop or published application after the user authenticates to the server. This setting saves the user from selecting a remote desktop or published application from a list that contains only one item.
`-smartCardPIN` *PIN*	Specifies the PIN when an end user inserts a smart card to log in.
`-usernameHint` *user_name*	Specifies the account name to use as the user name hint.
`-standalone`	Starts a second instance of Horizon Client that can connect to the same or a different server. This option is supported for backwards compatibility. Specifying `-standalone` is not necessary as it is the default behavior for the client. For multiple remote desktop connections to the same or a different server, using the secure tunnel is supported. **Note** The second remote desktop connection might not have access to the local hardware, such as USB devices, smart, cards, printers, and multiple monitors.
`-supportText` *file_name*	Specifies the full path of a text file. The content of the file is displayed in the About dialog box.
`-unattended`	Starts Horizon Client in a noninteractive mode that is suitable for clients in kiosk mode. You must also specify the following information: ■ The account name of the client, if you did not generate the account name from the MAC address of the client device. The name must begin with the string “custom-”, or an alternate prefix that you have configured in ADAM. ■ The password of the client, if you did not generate a password automatically when you set up the account for the client. The `-unattended` option implicitly sets the `-nonInteractive`, `-connectUSBOnStartup`, `-connectUSBOnInsert` , and `-desktopLayout multimonitor`options.

Table 3-14. Horizon Client Command-Line Options (continued)

Option	Description

`-unauthenticatedAccessAccount`	Specifies an Unauthenticated Access user account to use to log in anonymously to the server when Unauthenticated Access is enabled. If Unauthenticated Access is not enabled, this option is ignored.
	For example:
	`vmware-view.exe -serverURL view.mycompany.com`
	`-unauthenticatedAccessEnabled true`
	`-unauthenticatedAccessAccount anonymous1`

`-unauthenticatedAccessEnabled`	When set to `true`, enables Unauthenticated Access. If Unauthenticated Access is not available, the client can fall back to another authentication method. The **Unauthenticated Access** setting is visible, disabled, and selected in Horizon Client. When set to `false`, requires you to enter your credentials to log in and access your applications. The **Unauthenticated Access** setting is hidden and deselected in Horizon Client. If you do not specify this option, you can enable Unauthenticated Access in Horizon Client. The **Unauthenticated Access** setting is visible, enabled, and deselected.

`-useExisting`	Enables you to start multiple remote desktops and published applications from a single Horizon Client session.
	When you specify this option, Horizon Client determines whether a session that has the same user name, domain, and server URL exists and, if it does, reuses that session instead of creating a session.
	For example, in the following command, user-1 starts the Calculator application and a new session is created.
	`vmware-view.exe -userName user-1 -password secret`
	`-domainName domain -appName Calculator`
	`-serverURL view.mycompany.com -useExisting`
	In the next command, user1 starts the Paint application with the same user name, domain, and server URL, and the same session is used.
	`vmware-view.exe -userName user-1 -password secret`
	`-domainName domain -appName Paint`
	`-serverURL view.mycompany.com -useExisting`

`-userName` *user_ name*	Specifies the account name that the end user uses to log in to Horizon Client. If you generate the account name from the MAC address of the client device, you do not need to specify this option for clients in kiosk mode.

You can specify all options by Active Directory group policies, except for `-file`, `-languageId`, `-printEnvironmentInfo`, `-smartCardPIN`, and `-unattended`.

Note Group policy settings take precedence over settings that you specify from the command line. The command-line options are case sensitive.

Horizon Client Configuration File

You can read command-line options for Horizon Client from a configuration file.

You can specify the path of the configuration file as an argument to the `-file` *file_path* option of the `vmware-view` command. The file must be a Unicode (UTF-16) or ASCII text file.

Example: Example of a Configuration File for a Noninteractive Application

The following example shows the contents of a configuration file for a noninteractive application.

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

Example: Example of a Configuration File for a Client in Kiosk Mode

The following example shows a client in kiosk mode where the account name is based on the client's MAC address. The client has an automatically generated password.

```
-serverURL 145.124.24.100
-unattended
```

Using the Windows Registry to Configure Horizon Client

You can define default settings for Horizon Client in the Windows Registry instead of specifying these settings on the command line. Group policy settings take precedence over Windows Registry settings, and Windows Registry settings take precedence over the command line.

Note In a future version of Horizon Client, Windows registry settings might not be supported and group policy settings must be used.

The following table lists the registry settings for logging in to Horizon Client. These settings are located under `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\` in the registry. This location is specific to a particular user. The `HKEY_LOCAL_MACHINE` settings, which are described in the next table, are computer-wide settings and pertain to all local users and all domain users that have permission to log in to the computer in a Windows domain environment.

Table 3-15. Horizon Client Registry Settings for Credentials

Registry Setting	Description
`Password`	Default password.
`UserName`	Default user name.

The following table lists the registry settings for Horizon Client that do not include login credentials. The location of these settings depends on the type of system as follows:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\`
- For 64-bit Windows: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware VDM\Client\`

Table 3-16. Horizon Client Registry Settings

Registry Setting	Description
`DomainName`	Default NETBIOS domain name. For example, you might use `mycompany` rather than `mycompany.com`.
`EnableShade`	Determines whether the menu bar (shade) at the top of the Horizon Client window is enabled. The menu bar is enabled by default, except for clients in kiosk mode. A value of **`false`** disables the menu bar. **Note** This setting is applicable only when you have the display layout set to **All Monitors** or **Fullscreen**.
`ServerURL`	URL, IP address, or FQDN of the default Connection Server instance.
`EnableSoftKeypad`	If set to **`true`** and a Horizon Client window has focus, the physical keyboard, onscreen keyboard, mouse, and handwriting pad events are sent to the remote desktop or published application, even if the mouse or onscreen keyboard is outside the Horizon Client window. The default is **`false`**.

The following table shows security settings that you can add. The location of these settings depends on the type of system as follows:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- For 64-bit Windows: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware VDM\Client\Security`

Table 3-17. Security Settings

Registry Setting	Description and Valid Values
`CertCheckMode`	Certificate checking mode. Valid values are as follows: ■ **0** implements `Do not verify server identity certificates`. ■ **1** implements `Warn before connecting to untrusted servers`. ■ **2** implements `Never connect to untrusted servers`.
`SSLCipherList`	Configures the cipher list to restrict the use of certain cryptographic algorithms and protocols before establishing an encrypted TLS connection. The cipher list consists of one or more cipher strings separated by colons. All cipher strings are case-sensitive. The default value is **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. The default value means that TLS v1.1 and TLS v1.2 are enabled and SSL v.2.0, SSL v3.0, and TLS v1.0 are disabled. SSL v2.0, SSL v3.0, and TLS v1.0 are no longer the approved protocols and are permanently disabled. Cipher suites use 128-bit or 256-bit AES, remove anonymous DH algorithms, and sort the current cipher list in order of encryption algorithm key length. For reference information about the configuration, see http://www.openssl.org/docs/apps/ciphers.html .

The following table shows VMware Integrated Printing settings that you can configure. The location of these settings depends on the type of system as follows:

- For 32-bit Windows: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\PrintRedir`
- For 64-bit Windows: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware VDM\Client\PrintRedir`

Table 3-18. VMware Integrated Printing Settings

Registry Setting	Description and Valid Values
`EnableActualSizePrinting`	Determines whether to print files from a remote desktop by scaling and fitting the file contents to the printed page size or by printing the file contents at their actual size. Valid values are as follows: ■ **`true`** prints file contents at their actual size. ■ **`false`** scales and fits file contents to the printed page size. The default value is **`true`**.

Clearing the Last User Name Used to Log In to a Server

When end users log in to a Connection Server instance for which the **Hide domain list in client user interface** global setting is enabled, the **Domain** drop-down menu is hidden in Horizon Client and users provide domain information in the Horizon Client **User name** text box. For example, users must enter their user name in the format ***`domain\username`*** or ***`username@domain`***.

On a Windows client system, a registry key determines whether the last user name is saved and displayed in the **User name** text box the next time a user logs in to the server. To prevent the last user name from being displayed in the **User name** text box and exposing domain information, you must set the value of the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\dontdisplaylastusername` registry key to 1 on the Windows client system.

For information about hiding security information in Horizon Client, including the **Domain** drop-down menu and server URL information, see the topics about global settings in the *Horizon Administration* document.

Configure VMware Blast Options

You can configure VMware Blast options for remote desktop and published application sessions that use the VMware Blast display protocol.

You can allow H.264 decoding and High Efficiency Video Coding (HEVC). H.264 is an industry standard for video compression, which is the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. When H.264 decoding is allowed, you can also allow increased color fidelity.

The maximum resolution that is supported, and whether HEVC is supported, depends on the capability of the graphical processing unit (GPU) on the client. A GPU that can support 4K resolution for JPEG/PNG might not support 4K resolution for H.264. If a resolution for H.264 is not supported, Horizon Client uses JPEG/PNG instead.

If your environment uses a proxy server, you can specify whether to allow VMware Blast connections to an operating system proxy server.

For an SSL proxy server, you also need to configure certificate checking for secondary connections through the SSL proxy server. For more information, see Setting the Certificate Checking Mode in Horizon Client.

You can configure VMware Blast options before or after you connect to a server.

Prerequisites

To use High Efficiency Video Coding (HEVC), your environment must meet the following criterion:

- Horizon Agent 7.7 or later must be installed.
- For increased color accuracy with YUV 4:4:4, Horizon Agent 7.11 or later must be installed.
- Client system must have a GPU that supports HEVC decoding.
- For full range color and improved color fidelity, Horizon Agent 2203 or later and Horizon Client for Windows 2203 or later must be installed. These features apply only if YUV 4:4:4 is being used

The client-side **Allow Blast connections to use operating system proxy settings** group policy setting determines whether VMware Blast connections can connect through a proxy server and whether users can change the VMware Blast proxy server setting in the Horizon Client user interface. For more information, see Using Group Policy Settings to Configure Horizon Client.

Depending on the Horizon Agent version that is installed, a Horizon administrator can use agent-side group policy settings to enable or deactivate VMware Blast features, including H.264 and HEVC high color accuracy. For information, see "VMware Blast Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document.

Procedure

1 Start Horizon Client.

2 Click **Settings** (gear icon) in the upper-right corner of the menu bar and select **VMware Blast**.

3 To allow H.264 decoding in Horizon Client, toggle the **Allow H.264 Decoding** option to on.

   When this option is on (the default setting), Horizon Client uses H.264 decoding if the agent supports H.264 software or hardware encoding. If the agent does not support H.264 software or hardware encoding, Horizon Client uses JPG/PNG decoding (with Horizon Agent 7.x), or Blast Codec decoding (with Horizon Agent 2006 and later). When this option is deselected, Horizon Client uses JPG/PNG decoding (with Horizon Agent 7.x), or Blast Codec decoding (with Horizon Agent 2006 and later).

4 To allow increased color fidelity when H.264 decoding is allowed in Horizon Client, select the **Allow High Color Accuracy (reduces battery life and performance)** check box.

   When this option is selected, Horizon Client uses high color accuracy, but only if the agent supports high color accuracy. Selecting this option might reduce battery life and performance. This feature is deactivated by default.

5 To allow HEVC, toggle the **Allow High Efficiency Video Decoding (HEVC)** option to on.

   When this option is selected, performance and image quality are improved if the client machine has a GPU that supports HEVC decoding. This feature is enabled by default.

   If this option is selected but the client machine does not have a GPU that supports HEVC decoding, or the agent does not support HEVC encoding, Horizon Client uses H.264 decoding instead if H.264 is selected. Horizon Client uses Blast Codec decoding if H.264 is not selected.

6 To enable high dynamic range decoding, select the **Allow High Dynamic Range Decoding (HDR)** check box.

   This option is available only if you enable the **Allow High Efficiency Video Decoding (HEVC)** setting.

7 To allow VMware Blast connections through a proxy server, toggle the **Allow Blast connections to use operating system proxy settings** option to on.

Results

Changes take effect the next time a user connects to a remote desktop or published application and selects the VMware Blast display protocol. Your changes do not affect existing VMware Blast sessions.

Using Internet Explorer Proxy Settings

Horizon Client uses proxy settings configured in Internet Explorer.

Bypassing Proxy Settings

Horizon Client uses the Internet Explorer proxy bypass settings to bypass HTTPS connections to a Connection Server host, security server, or Unified Access Gateway appliance.

If the secure tunnel is enabled on the Connection Server host, security server, or Unified Access Gateway appliance, you must use the `Tunnel proxy bypass address list` group policy setting in the Horizon Client Configuration ADM or ADMX template file to specify a list of addresses to bypass the tunnel connection. The proxy server is not used for these addresses. Use a semicolon (;) to separate multiple entries. This group policy setting creates the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

You cannot use this group policy setting for direct connections. If applying the group policy setting does not work as expected, try bypassing the proxy for local addresses. For more information, see https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem-is-not-available/.

Proxy Fail Over

Horizon Client supports proxy fail over with the **Use automatic configuration script** setting under **Automatic configuration** in **Internet Options > Connections > LAN settings** in Internet Explorer. To use this setting, you must create an automatic configuration script that returns multiple proxy servers.

Configure Horizon Client Data Sharing

If a Horizon administrator has opted to participate in the VMware Customer Experience Improvement Program (CEIP), VMware collects and receives anonymous data from client systems through Connection Server. You can configure whether to share this client data with Connection Server.

For information about configuring Horizon to join the CEIP, see the *Horizon Administration* document.

Data sharing is enabled by default in Horizon Client. You must configure the data sharing setting before you connect to a server. The setting is applied to all servers. You cannot change the Horizon Client data sharing setting after you connect to a server.

You can use the **Allow data sharing** group policy setting to enable or disable data sharing and prevent users from changing the setting in Horizon Client. For more information, see Using Group Policy Settings to Configure Horizon Client.

VMware collects data about client systems to prioritize hardware and software compatibility. If your Horizon administrator has opted to participate in the customer experience improvement program, VMware collects anonymous data about your deployment to respond better to customer requirements. VMware does not collect data that identifies your organization. Horizon Client information is sent first to the Connection Server instance and then to VMware, along with data about Connection Server, desktop pools, and remote desktops.

The information is encrypted when it is in transit to the Connection Server instance. The information on the client system is logged unencrypted in a user-specific directory. The logs do not contain personally identifiable information.

A Horizon administrator can select whether to participate in the VMware customer experience improvement program when installing Connection Server or by setting an option in Horizon Console after the installation.

Table 3-19. Data Collected from Horizon Clients for the Customer Experience Improvement Program

Description	Is This Field Made Anonymous?
Company that produced the Horizon Client application	No
Product name	No
Client product version	No
Client binary architecture	No
Client build name	No
Host operating system	No
Host operating system kernel	No
Host operating system architecture	No
Host system model	No
Host system CPU	No
Number of cores in the host system's processor	No
MB of memory on the host system	No
Number of USB devices connected	No
Maximum concurrent USB device connections	No

Table 3-19. Data Collected from Horizon Clients for the Customer Experience Improvement Program (continued)

Description	Is This Field Made Anonymous?
USB device vendor ID	No
USB device product ID	No
USB device family	No
USB device use count	No

Procedure

1 Start Horizon Client.

2 Click **Settings** (gear icon) in the upper-right corner of the menu bar and select **Data Sharing**.

3 Toggle the **Data sharing mode** option to on or off.

MAC Address Deny List

Horizon Client reports the MAC address of the user's local hardware instead of the MAC address of the VPN by using a hard-coded deny list of MAC addresses.

The following MAC addresses are included in the deny list.

```
000000000000
00059a3c7800
00059a3c7a00
00090faa0001
00090ffe0001
001c42000008
001c42000009
005056c00001
005056c00008
00ff091cb893
00ff10404c08
00ff39c549ca
00ff5ab2e94a
00ff5d79fab3
00ffa43eb222
00ffc7cd3234
02004c4f4f50
0205857feb80
025041000001
080027000443
080027000c04
0800270014be
080027002049
08002700281e
080027003494
0800270034f0
080027004816
```

```
08002700509c
0800270074bd
08002700802d
08002700ac25
08002700c4be
08002700c84c
08002700c84e
08002700d49e
08002700e41d
08002700e4a0
08002700e843
08002700e865
08002700e8d3
08002700f061
08002700f091
08002700f4eb
0a0027000000
0a0027000002
0a0027000003
0a002700000d
1e85de8f5e73
2e85de8f5e73
```

In addition, the following MAC address is used for the Touch Bar on many MacBook laptops.

```
acde48001122
```

Managing Remote Desktop and Published Application Connections

4

End users can use Horizon Client to connect to a server, log in to or off of remote desktops, and use published applications. For troubleshooting purposes, end users can also restart and reset remote desktops and reset published applications.

Depending on how you configure policies, end users might be able to perform many operations on their remote desktops and published applications.

This chapter includes the following topics:

- Connect to a Remote Desktop or Published Application
- Use Unauthenticated Access to Connect to Published Applications
- Share Location Information
- Hide the VMware Horizon Client Window
- Reconnecting to a Remote Desktop or Published Application
- Create a Shortcut on the Windows Client Desktop or in the Start Menu
- Configure Start Menu Shortcut Updates
- Configure the Autoconnect Feature for a Remote Desktop
- Log Off or Disconnect
- Disconnecting From a Server

Connect to a Remote Desktop or Published Application

To connect to a remote desktop or published application, you must provide the name of a server and supply credentials for your user account.

Before you have end users access their remote desktops and published applications, test that you can connect to a remote desktop or published application from a client device. You might need to specify a server and supply credentials for your user account.

Prerequisites

- Obtain login credentials, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication credentials, or smart card personal identification number (PIN).
- Obtain the NETBIOS domain name for logging in. For example, you might use `mycompany` rather than `mycompany.com`.
- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.
- If you are outside the corporate network and require a VPN connection to access remote desktops and published applications, verify that the client device is set up to use a VPN connection and turn on that connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the remote desktop or published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- If you plan to use the RDP display protocol to connect to a remote desktop, verify that the AllowDirectRDP agent group policy setting is enabled. For information, see the *Configuring Remote Desktop Features in Horizon* document.
- Configure the certificate checking mode for the certificate presented by the server. To determine which mode to use, see Setting the Certificate Checking Mode in Horizon Client.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Start Horizon Client.
3. (Optional) To log in as the currently logged-in Windows domain user, click the **Options** menu (… icon) in the upper-right corner of the menu bar and select **Log in As Current User**.

   This setting is available only if the **Log in as current user** feature is installed on the client system.
4. Connect to a server.

Option	Action
Connect to a new server	Click the **+ Add Server** button, or click **+ Add Server** on the menu bar, enter the name of a server, and click **Connect**. **Note** To specify an IPv6 address when adding a server, you must wrap the address in square brackets.
Connect to an existing server	Double-click the server icon, or right-click the server icon and select **Connect**.

Connections between Horizon Client and the server always use TLS. The default port for TLS connections is 443. If the server is not configured to use the default port, use the format *`servername`*`:`*`port`*, for example, **`view.company.com:1443`**.

You might see a message that you must confirm before the login dialog box appears.

5 If you are prompted for RSA SecurID credentials or RADIUS authentication credentials, enter the credentials and click **Continue**.

6 Enter the credentials of a user who is entitled to use at least one remote desktop or published application, select the domain, and click **Login**.

If you enter the user name as **`username@domain`**, Horizon Client treats it as a user principal name (UPN) and the **Domain** drop-down menu is disabled.

If the **Domain** drop-down menu is hidden, you must enter the user name as ***`username`***`@`***`domain`*** or ***`domain\username`***.

7 If Horizon Client prompts you to create shortcuts to published applications or remote desktops in your **Start** menu or on the remote desktop, click **Yes** or **No**.

This prompt can appear the first time you connect to a server on which shortcuts have been configured for published applications or remote desktops. If you click **Yes**, **Start** menu shortcuts or desktop shortcuts are installed on the client system for those published applications or remote desktops, if you are entitled to use them. If you click **No**, **Start** menu or desktop shortcuts are not installed.

A Horizon administrator can configure the **Automatically install shortcuts when configured on the Horizon server** group policy setting to prompt end users to install shortcuts (the default), install shortcuts automatically, or never install shortcuts.

8 (Optional) To configure display settings for a remote desktop, right-click the remote desktop icon and select **Settings**.

Option	Action
Select a display protocol	If a Horizon administrator has allowed it, use the **Connect Via** drop-down menu to select the display protocol.
Select a display layout	Use the **Display** drop-down menu to select a window size or to use multiple monitors.

9 To connect to a remote desktop or published application, double-click the remote desktop or published application icon in the desktop and application selection window.

If you are connecting to a published desktop, and if the published desktop is already set to use a different display protocol, you cannot connect immediately. Horizon Client prompts you to use the set protocol or to log off so that Horizon Client can connect with a different display protocol.

Results

After you are connected, the remote desktop or published application opens.

If you are entitled to more than one remote desktop or published application on the server, the desktop and application selector window remains open so that you can connect to multiple remote desktops and published applications.

If the client drive redirection feature is enabled, the Sharing dialog box appears and you can allow or deny access to files on the local file system. For more information, see Share Local Folders and Drives.

The first time you connect to a server, Horizon Client saves a shortcut to the server on the Horizon Client home window. You can double-click this server shortcut the next time you need to connect to the server.

If authentication to the server fails, or if the client cannot connect to the remote desktop or published application, perform the following tasks:

- Verify that the certificate for the server is working properly. If it is not, in Horizon Console, you might also see that the agent on remote desktops is unreachable. These symptoms indicate additional connection problems caused by certificate problems.
- Verify that the tags set on the Connection Server instance allow connections from this user. See the *Horizon Administration* document.
- Verify that the user is entitled to access this remote desktop or published application. See the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.
- If you are using the RDP display protocol to connect to a remote desktop, verify that the remote desktop operating system allows remote desktop connections.

What to do next

Configure startup settings. If you do not want to require end users to provide the host name of the server, or if you want to configure other startup settings, use a command-line option to create a remote desktop shortcut. See Running Horizon Client From the Command Line.

Use Unauthenticated Access to Connect to Published Applications

If you have an Unauthenticated Access user account, you can log in to a server anonymously and connect to your published applications.

Before you have end users access a published application with the Unauthenticated Access feature, test that you can connect to the published application from a client device. You might need to specify a server and supply credentials for your user account.

By default, users select the **Unauthenticated Access** setting from the **Options** menu and select a user account to log in anonymously. A Horizon administrator can configure group policy settings to preselect the **Unauthenticated Access** setting and log in users with a specific Unauthenticated Access user account.

Prerequisites

- Perform the administrative tasks described in Preparing Connection Server for Horizon Client.
- Set up Unauthenticated Access users on the Connection Server instance. For information, see "Providing Unauthenticated Access for Published Applications" in the *Horizon Administration* document.
- If you are outside the corporate network, verify that your client device is set up to use a VPN connection and turn on that connection.
- Verify that you have the fully qualified domain name (FQDN) of the server that provides access to the published application. Underscores (_) are not supported in server names. If the port is not 443, you also need the port number.
- Configure the certificate checking mode for the certificate presented by the server in Horizon Client. To determine which mode to use, see Setting the Certificate Checking Mode in Horizon Client.
- (Optional) Configure the **Account to use for Unauthenticated Access** and **Enable Unauthenticated Access to the server** group policy settings to change the default Unauthenticated Access behavior. For information, see Using Group Policy Settings to Configure Horizon Client.

Procedure

1. If a VPN connection is required, turn on the VPN.
2. Start Horizon Client.
3. Click **Options** in the menu bar and select **Unauthenticated Access**.

   Depending on how the client system is configured, this setting might be preselected.

4. Connect to the server on which you have unauthenticated access.

Option	Action
Connect to a new server	Click the **+ Add Server** button, or click the **+ Add Server** button in the menu bar, enter the name of the server, and click **Connect**.
Connect to an existing server	Double-click the server icon on the Horizon Client home window.

   Connections between Horizon Client and the server always use TLS. The default port for TLS connections is 443. If the server is not configured to use the default port, use the format shown in this example: **`view.company.com:1443`**.

   You might see a message that you must confirm before the Login dialog box appears.

5. When the Login dialog box appears, select an account from the **User account** drop-down menu, if necessary.

   If only one user account is available, the drop-down menu is disabled and the user account is preselected.

6 (Optional) If the **Always use this account** check box is available, select it to bypass the Login dialog box the next time you connect to the server.

   To deselect this setting before you connect to the server the next time, right-click the server icon on the Horizon Client home window and select **Wipe Unauthenticated Account**.

7 Click **Login** to log in to the server.

   The application selector window appears.

8 To start a published application, double-click the published application icon.

Share Location Information

This topic describes how to share location information of a client system.

When connecting to a remote desktop or published application, you can share the client system's location information using the Geolocation Redirection feature or with Microsoft Teams Optimization. For Geolocation Redirection, you must enable the feature. For Microsoft Teams Optimization, location information sharing (E911) is enabled by default. In addition to sharing the client system's information, you must also configure a setting in Horizon Client.

Prerequisites

For the Geolocation Redirection feature, a Horizon administrator must configure the Geolocation Redirection feature for the remote desktop or published application. Complete the following steps for this task:

- Enable the Geolocation Redirection feature when you install Horizon Agent.
- Set group policies to configure Geolocation Redirection features.
- Enable the VMware Horizon Geolocation Redirection IE Plugin.

For complete requirements, see System Requirements for Geolocation Redirection.

To use Microsoft Teams Optimization, you must enable this feature. Enabling Microsoft Teams Optimization also enables E911 (location sharing). For complete requirements, see Configure E911 Services for Microsoft Teams.

Procedure

1 Using Horizon Client, connect to a server and open **Settings**.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window.
   - Right-click a remote desktop or published application in the desktop and application selector window and select **Settings**.

2 Configure the geolocation settings and click **Back** (**<**).

Option	Action
Share the client system's location information with remote desktops and published applications	Toggle the **Share your location** option to on.
Do not show the Geolocation dialog box when you connect to a remote desktop or published application	Select the **Do not show dialog when connecting a desktop or application** check box. The Geolocation dialog box asks you whether you want to share location information with a remote desktop or published application. If this check box is deselected, the Geolocation dialog box appears the first time you connect to a remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Geolocation dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box again. To see the dialog box again, you must disconnect from the server and log in again.

Hide the VMware Horizon Client Window

You can hide the VMware Horizon Client window after you open a remote desktop or published application.

You can use a group policy setting to configure whether the window is always hidden after a remote desktop or published application opens. For more information, see Using Group Policy Settings to Configure Horizon Client.

Procedure

- To hide the VMware Horizon Client window after you open a remote desktop or published application, click the **Close** button in the corner of the VMware Horizon Client window.
- To show the desktop from the client, from a remote desktop, or a published application, press Window key + D.
- To change focus to another window from the client, a remote desktop, or a published application, press Alt + Tab.
- To configure a setting that always hides the VMware Horizon Client window after a remote desktop or published application opens, before you connect to a server, click **Options** in the menu bar and select **Hide Selector After Launching**.
- To show the VMware Horizon Client window after it has been hidden, right-click the VMware Horizon Client icon in the system tray and select **Show VMware Horizon Client**.

Reconnecting to a Remote Desktop or Published Application

For security purposes, a Horizon administrator can set timeouts that log you off a server and lock a published application after some period of inactivity.

By default, you must log in again if you have Horizon Client open and are connected to a particular server for more than 10 hours. This timeout applies to both remote desktop and published application connections.

You receive a warning prompt 30 seconds before a published application is locked automatically. If you do not respond, the published application is locked. By default, the timeout occurs after 15 minutes of inactivity, but a Horizon administrator can change the timeout period.

For example, if you have one or more published applications open and you walk away from your computer, the published application windows might no longer be open when you return an hour later. Instead, you might see a dialog box that prompts you to click **OK** to re-authenticate to the server so that the published applications windows appear again.

To configure these timeout settings in Horizon Console, select **Settings > Global Settings**, click the **General Settings** tab, and click **Edit**.

Create a Shortcut on the Windows Client Desktop or in the Start Menu

You can create a shortcut for a remote desktop or published application. The shortcut appears on the client system's desktop, just like shortcuts for locally installed applications. You can also create a Windows Start menu shortcut.

Procedure

1. Start Horizon Client and log in to the server.
2. In the desktop and application selector window, right-click a remote desktop or published application and select **Create Shortcut to Desktop** or **Add to Start Menu** from the context menu.

Results

Depending on the command that you selected, Horizon Client creates a shortcut on the desktop or in the Windows Start menu on the client system.

What to do next

You can rename, delete, or perform any action on a shortcut that you can perform on shortcuts for locally installed applications. If you are not already logged in to the server when you use the shortcut, Horizon Client prompts you to log in before the remote desktop or published application opens.

Configure Start Menu Shortcut Updates

A Horizon administrator might configure Start menu or desktop shortcuts for certain remote desktops and published applications. You can configure whether changes made to remote desktop and published application shortcuts on the server are applied to the client system when you connect to the server.

If you are entitled to a remote desktop or published application that has shortcuts, Horizon Client places the shortcuts in the Start menu, on the desktop, or both, on the client system when you connect to the server.

On Windows 10 systems, Horizon Client places shortcuts in the Apps list. If a Horizon administrator creates a category folder for a shortcut, the category folder appears under the VMware Applications folder or as a category in the Apps list.

You can use a group policy setting to configure whether Horizon Client installs shortcuts automatically, prompts end users before installing shortcuts, or never installs shortcuts. For more information, see the **Automatically install shortcuts when configured on the Horizon server** group policy setting in Using Group Policy Settings to Configure Horizon Client.

You can use the `vmware-view` command with the `-installShortcutsThenQuit` option to create a script that runs when the client system starts up and installs shortcuts automatically. For more information, see Running Horizon Client From the Command Line .

If you are not already logged in to the server when you click a server-created shortcut, Horizon Client prompts you to log in before the remote desktop or published application opens.

If a Horizon administrator modifies remote desktop and published application shortcuts on the server, by default the shortcuts are updated on the client system the next time you connect to that server. You can change the default shortcut update behavior in Horizon Client. For more information, see Configure Start Menu Shortcut Updates.

To remove server-created shortcuts from the client system, you can delete the server from the Horizon Client server selection window or uninstall Horizon Client.

Note Users are not prompted to install server-created shortcuts, and server-created shortcuts are not created, on clients in kiosk mode.

Prerequisites

You cannot change the shortcut update setting unless you have previously installed a shortcut from a server.

Procedure

1. Start Horizon Client and connect to a server.
2. Open the **Settings** dialog box and select **Shortcuts**.
   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window.
   - Right-click the remote desktop or published application icon and select **Settings**.
3. Toggle the **Automatically update list of application and desktop shortcuts** option to on or off.

Configure the Autoconnect Feature for a Remote Desktop

You can configure a server to open a particular remote desktop automatically when you connect to that server. You cannot configure a server to open a published application automatically.

Prerequisites

Obtain credentials for connecting to the server, such as a user name and password, RSA SecurID user name and passcode, RADIUS authentication user name and passcode, or smart card personal identification number (PIN).

Procedure

1. Start Horizon Client and connect to the server.
2. In the desktop and application selector window, select the remote desktop, select **Settings** (gear icon) in the upper-right corner of the window, and toggle the **Autoconnect to this desktop** option to on.
3. Disconnect from the server.
4. Reconnect to the server.

   Horizon Client launches the remote desktop automatically.
5. (Optional) If you need to disable the autoconnect feature for the remote desktop, in the desktop and application selector window, select the remote desktop, select **Settings** (gear icon) in the upper-right corner of the window, and toggle the **Autoconnect to this desktop** option to off.

Log Off or Disconnect

If you disconnect from a remote desktop without logging off, applications in the remote desktop might remain open. You can also disconnect from a server and leave published applications running.

You can log off from a remote desktop even if you do not have the remote desktop open. This feature has the same result as sending Ctrl+Alt+Del to the remote desktop and then clicking **Log Off**.

Note The Windows key combination Ctrl+Alt+Del is not supported in remote desktops. Instead, click the **Ctrl+Alt+Delete** button in the menu bar. Alternatively, you can press Ctrl+Alt+Insert.

Procedure

- Disconnect from a remote desktop without logging off.

Option	Action
From the remote desktop window	Perform one of the following actions: ■ Click the **Close** button in the corner of the remote desktop window. ■ Select **Options** from the menu bar in the remote desktop window and select **Disconnect**.
From the desktop and application selector window	In the upper-left corner of the desktop and application selector window, click the **Disconnect from this server** icon and click **OK** in the warning dialog box. If you are entitled to multiple remote desktops or published applications on the server, the desktop and application selector window is open.

Note A Horizon administrator can configure remote desktops to log off when they are disconnected. In that case, any open applications in the remote desktop are closed.

- Log off and disconnect from a remote desktop.

Option	Action
From within the remote desktop	Use the Windows **Start** menu to log off.
From the menu bar	Select **Options** and select **Logoff Desktop**. If you use this procedure, files that are open on the remote desktop are closed without being saved first.

- Disconnect from a published application.

Option	Action
Disconnect from the published application but not the server	Quit the published application in the usual manner, for example, click the **Close** button in the corner of the application window.
Disconnect from the published application and the server	In the upper-left corner of the application selector window, click the **Disconnect from this server** icon and click **OK** in the warning dialog box.
Close the application selector window, but leave the published application running	Click the **Close** button. The application selector window closes.

- Log off when you do not have a remote desktop open.

  If you use this procedure, files that are open on the remote desktop are closed without being saved first.

  a Start Horizon Client, connect to the server that provides access to the remote desktop, and supply authentication credentials.

  b Right-click the remote desktop icon and select **Logoff**.

Disconnecting From a Server

After you have finished using a remote desktop or published application, you can disconnect from the server.

To disconnect from a server, click the **Disconnect from this server** icon in the upper-left corner of the Horizon Client window.

Working in a Remote Desktop or Published Application

5

Horizon Client for Windows provides a familiar, personalized desktop and application environment. End users can access USB and other devices connected to their local Windows computer, send documents to any printer that their local computer can detect, use smart cards to authenticate, and use multiple display monitors.

This chapter includes the following topics:

- Feature Support for Windows Clients
- Resizing the Remote Desktop Window
- Supported Multiple Monitor Configurations
- Select Specific Monitors to Display a Remote Desktop
- Display a Remote Desktop on a Single Monitor in a Multiple-Monitor Setup
- Select Specific Monitors to Display Published Applications
- Use Display Scaling
- Using DPI Synchronization
- Change the Display Mode for a Remote Desktop
- Customize the Display Resolution and Display Scaling for a Remote Desktop
- Use USB Devices
- USB Redirection Limitations
- Using Webcams and Microphones
- When You Can Use a Webcam with the Real-Time Audio-Video Feature
- Select a Preferred Webcam or Microphone on a Windows Client System
- Using Multiple Devices with the Real-Time Audio-Video Feature
- Select a Preferred Speaker for a Remote Desktop
- Sharing Remote Desktop Sessions
- Invite a User to Join a Remote Desktop Session
- Manage a Shared Remote Desktop Session

- Join a Remote Desktop Session
- Share Local Folders and Drives
- Open Local Files in Published Applications
- Copying and Pasting
- Logging Copy and Paste Activity
- Configuring the Client Clipboard Memory Size
- Dragging and Dropping
- Tips for Using Published Applications
- Reconnect to Published Applications After Disconnecting
- Use Multiple Sessions of a Published Application From Different Client Devices
- Use a Local IME with Published Applications
- Use a Local IME with a Remote Desktop
- Printing From a Remote Desktop or Published Application
- Set Printing Preferences for the VMware Integrated Printing Feature
- Printing From a Remote Desktop to a Local USB Printer
- Improve Mouse Performance in a Remote Desktop
- Using Scanners
- Redirecting Serial Ports
- Keyboard Shortcuts for Input Focus
- Keyboard Input Source Language Synchronization
- Configure Lock Key Synchronization

Feature Support for Windows Clients

Certain guest operating systems and remote desktop features require specific Horizon Agent versions. Use this information when planning which features to make available to your end users.

Supported Windows Virtual Desktops

Windows virtual desktops are single-session virtual machines.

This version of Horizon Client works with Windows virtual desktops that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows 7, Windows 8.x, and Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 virtual desktops require Horizon Agent 7.7 or later.

- Windows 7 and Windows 8.x virtual desktops are not supported with Horizon Agent 2006 and later.

Supported Published Desktops on RDS Hosts

RDS hosts are server computers that have Windows Remote Desktop Services and Horizon Agent installed. Multiple users can have published desktop sessions on an RDS host simultaneously. An RDS host can be either a physical machine or a virtual machine.

This version of Horizon Client works with RDS hosts that have Horizon Agent 7.5 or later installed. Supported guest operating systems include Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019, with the following limitations:

- Windows Server 2019 RDS hosts require Horizon Agent 7.7 or later.
- Window Server 2012 RDS hosts are not supported with Horizon Agent 2006 and later.

Requirements for Specific Remote Desktop Features

Most remote desktop features work with Horizon Agent 7.5, but some features require later Horizon Agent versions.

Feature	Requirements
Dragging text and images	Horizon Agent 7.9 or later
Dragging files and folders	Horizon Agent 7.7 or later
Geolocation Redirection	Horizon Agent 7.6 or later
Browser Redirection	Horizon Agent 7.10 or later
VMware Integrated Printing and location-based printing	Horizon Agent 7.7 or later

This version of Horizon Client for Windows does not support the following remote desktop features, which are supported in Horizon Agent 7.x releases:

- Virtual Printing (also known as ThinPrint)
- Flash URL Redirection
- Flash Redirection

Supported Linux Desktops

For a list of supported Linux guest operating systems and information about supported features, see the *Setting Up Linux Desktops in Horizon* document.

Resizing the Remote Desktop Window

If a Horizon administrator has locked the guest size, or if you are using the RDP display protocol, you cannot change the resolution of the remote desktop window.

If you have multiple monitors, you can select the monitors on which to display a remote desktop window. For more information, see Select Specific Monitors to Display a Remote Desktop. You can also configure the remote desktop window to open on a single monitor. For more information, see Display a Remote Desktop on a Single Monitor in a Multiple-Monitor Setup.

Supported Multiple Monitor Configurations

Horizon Client supports the following multiple monitor configurations.

- With the VMware Blast display protocol, beginning with Horizon 7 version 7.8, six monitors at 2560 X 1600 resolution with virtual desktops that are running Windows 10 version 1703 or later are supported. Updated Windows display specifications require Windows 10 version 1803 or later for six monitor support on Horizon 7 version 7.9 and later.
- With instant clone desktop pools, the maximum number of monitors is four at 4K resolution.
- With two or more monitors, the monitors are not required to be in the same mode. For example, if you are using a laptop connected to an external monitor, the external monitor can be in portrait mode or landscape mode.
- With Hardware Version 13 or earlier, monitors can be placed side by side, stacked two by two, or vertically stacked only if you are using two monitors and the total height is less than 4096 pixels.
- To use the selective multiple-monitor feature, you must use the VMware Blast display protocol or the PCoIP display protocol. For more information, see Select Specific Monitors to Display a Remote Desktop and Select Specific Monitors to Display Published Applications.
- To use the vSGA 3D rendering feature, you must use the VMware Blast display protocol or the PCoIP display protocol. You can use up to two monitors, with a resolution of up to 1920 X 1200. For a resolution of 4K (3840 X 2160), only one monitor is supported.
- For vGPU or other GPU passthrough modes, the vendor hardware and drivers determine the number of monitors and maximum resolution. For more information, see the *NVIDIA GRID Virtual GPU User Guide*, or go to the vendor website.
- If you are using five or more monitors, and you connect to a remote session with VMware Blast, if you use the same user credentials to connect to the session with PCoIP from a different device (without logging off the original session), the initial connection to the new session fails.
- With the VMware Blast display protocol, a remote desktop screen resolution of 8K (7680 x 4320) is supported. Two 8K displays are supported. The hardware version of the desktop virtual machine must be 14 (ESXi 6.7 or later). You must allocate sufficient system resources in the virtual machine to support an 8K display. For information about supported monitor configurations for GRID-based desktops, and for NVIDIA vGPU profiles, see the *Virtual GPU Software User Guide* on the NVIDIA website. This feature is supported only with the Windows client.

- With the VMware Blast display protocol or the PCoIP display protocol, a remote desktop screen resolution of 4K (3840 x 2160) is supported. The number of 4K displays that are supported depends on the hardware version of the desktop virtual machine and the Windows version.

Hardware Version	Windows Version	Number of 4K Displays Supported
10 (ESXi 5.5.x compatible)	7, 8, 8.x, 10	1
11 (ESXi 6.0 compatible)	7 (3D rendering feature disabled and Windows Aero disabled)	3
11	7 (3D rendering feature enabled)	1
11	8, 8.x, 10	1
13 or 14	7, 8, 8.x, 10 (3D rendering feature enabled)	1
13 or 14	7, 8, 8.x, 10	4

  For the best performance, the virtual machine should have at least 2 GB of RAM and 2 vCPUs. This feature might require good network conditions, such as a bandwidth of 1000 Mbps with low network latency and a low package loss rate.

  Note When the remote desktop screen resolution is set to 3840 x 2160 (4K), items on the screen might appear smaller, and you might not be able to use the Screen Resolution dialog box in the remote desktop to make text and other items larger. In this scenario, you can set the client machine's DPI to the proper setting and enable the DPI Synchronization feature to redirect the client machine's DPI setting to the remote desktop.

- If you use Microsoft RDP 7, the maximum number of monitors that you can use to display a remote desktop is 16.
- If you use the Microsoft RDP display protocol, you must have Microsoft Remote Desktop Connection (RDC) 6.0 or later installed in the remote desktop.

Select Specific Monitors to Display a Remote Desktop

If you have two or more monitors, you can select the monitors on which to display a remote desktop window. For example, if you have two monitors, you can specify that the remote desktop window appears on only one of those monitors.

Beginning with Horizon 7 version 7.8, you can select up to six adjacent monitors with virtual desktops that are running Windows 10 version 1703 and later. Beginning with Horizon 7 version 7.9, you can select up to six adjacent monitors with virtual desktops that are running Windows 10 version 1803 and later. The monitors can be side by side, or stacked vertically. For example, you might configure two rows of three monitors each. With other Windows versions, or earlier VMware Horizon releases, you can use up to four adjacent monitors.

Prerequisites

You must have two or more monitors.

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box for the remote desktop.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.
   - Right-click the remote desktop in the desktop and application selection window and select **Settings**.

3 Select **PCoIP** or **VMware Blast** from the **Connect Via** drop-down menu.

   The **Connect Via** drop-down menu appears only if a Horizon administrator has enabled it.

4 From the **Display** drop-down menu, select **Fullscreen - All Monitors**.

   Thumbnails of the monitors that are currently connected to the client system appear under Display settings. The display topology matches the display settings on the client system.

5 To select or deselect a monitor on which to display the remote desktop window, click a thumbnail.

   When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.

6 To save your changes, click **Apply**.

7 Connect to the remote desktop.

   Your changes are applied immediately when you connect to the remote desktop. Horizon Client saves display settings in a preferences file for the remote desktop after you exit from Horizon Client.

Display a Remote Desktop on a Single Monitor in a Multiple-Monitor Setup

If you have two or more monitors, but you want a remote desktop window to appear on only one monitor, you can configure the remote desktop window to open on a single monitor.

Prerequisites

You must have two or more monitors.

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box for the remote desktop.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.
   - Right-click the remote desktop in the desktop and application selection window and select **Settings**.

3 From the **Connect Via** drop-down menu, select **VMware Blast**, **PCoIP**, or **Microsoft RDP**.

4 From the **Display** drop-down menu, select **Fullscreen - Single Monitor** , **Window - Large**, **Window - Small**, or **Custom**.

   Window - Large maximizes the window size. **Window - Small** sets the window size to 640 x 480 pixels in 100 percent scaling. If you select **Custom**, you can select a specific window size.

Results

By default, the remote desktop window opens on the primary monitor. You can drag the remote desktop window to a non-primary monitor, and the next time you open the remote desktop, the remote desktop window appears on that same monitor. The window opens, is centered in the monitor, and uses the window size that you selected for the display mode, not a size that you might have created by dragging the window to resize it.

Select Specific Monitors to Display Published Applications

If you have two or more monitors, you can select the monitors on which to display published application windows. For example, if you have two monitors, you can specify that published application windows appear on only one of those monitors.

You can select up to four adjacent monitors. The monitors can be side by side, stacked two by two, or stacked vertically. A maximum of two monitors can be stacked vertically.

Prerequisites

You must have two or more monitors.

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box for published applications.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select **Applications**.
   - Right-click a published application in the desktop and application selection window and select **Settings**.

3 Under Display Settings, select or deselect a monitor on which to display the published application window.

   When you select a monitor, its thumbnail changes color. If you violate a display selection rule, a warning message appears.

4 To save your changes, click **Apply**.

Use Display Scaling

Users that have poor eyesight or high-resolution screens, such as 4K monitors, generally have scaling enabled by setting the DPI (Dots Per Inch) on the client system to greater than 100 percent. The DPI setting controls the size of the text, apps and icons. A lower DPI setting makes them appear smaller and a higher setting makes them appear bigger. With the Display Scaling feature, remote desktops and published applications support the client system's scaling setting and appear normal-sized rather than very small.

Horizon Client compares the DPI setting that it receives from the remote desktop or published application to the client system's DPI setting. If the DPI settings do not match, and the Display Scaling feature is enabled, Horizon Client calculates the scale factor. For example, if a remote desktop's DPI setting is 100 percent and the client system's DPI setting is 200 percent, Horizon Client scales up the remote desktop's DPI setting by a factor of 2 (200 / 100 = 2) .

Horizon Client saves the display scaling setting for each remote desktop separately. For published applications, the display scaling setting applies to all published applications that are available to the currently logged-in user.

In a multiple-monitor setup, using display scaling does not affect the number of monitors and the maximum resolutions that Horizon Client supports. When display scaling is allowed and is in effect, scaling is based on the client system's DPI setting.

You can hide the display scaling setting by enabling the Horizon Client **Locked Guest Size** group policy setting.

You can enable or disable display scaling for all remote desktops and published applications by setting the **Allow display scaling** group policy setting. For information, see Using Group Policy Settings to Configure Horizon Client. **Allow display scaling** is enabled by default and the option is turned on in the user interface.

Procedure

1 Start Horizon Client and connect to a server.

2 In the desktop and application selector window, right-click the remote desktop or published application and select **Settings**.

3 Toggle the **Allow display scaling** option to on.

   If an administrator has preconfigured display scaling, the check box is dimmed. If an administrator has hidden the display scaling setting, the check box does not appear.

Using DPI Synchronization

The DPI Synchronization feature ensures that the DPI setting in a remote desktop or published application matches the client system's DPI setting.

Like the Display Scaling feature, the DPI Synchronization feature can improve the readability of text and icons on high-DPI displays. Unlike the Display Scaling feature, which increases the size of fonts and images and can make them blurry, the DPI Synchronization feature increases the size of fonts and images, keeping them sharp. For this reason, the DPI Synchronization feature is generally preferred for an optimal user experience.

If the DPI Synchronization feature and the Display Scaling feature are both enabled, only one feature takes effect at any given time.

The **DPI Synchronization** agent group policy setting determines whether the DPI Synchronization feature is enabled. The feature is enabled by default.

Behavior of DPI Synchronization with Remote Desktops

The default DPI synchronization behavior depends on the Horizon Agent version that is installed in the agent machine.

Beginning with Horizon Agent 2012, the client's per-monitor DPI setting is synchronized to the agent and changes take effect immediately during a remote session by default. This feature is controlled by the **DPI Synchronization Per Monitor** agent group policy setting. The DPI Synchronization Per Monitor feature is supported by default for virtual desktops and physical desktops. It is not supported for published desktops.

With earlier Horizon Agent versions, Horizon Client supports synchronization only to the system DPI setting. DPI Synchronization happens during the initial connection, and Display Scaling works in case of reconnection, if necessary. When DPI Synchronization works and the client system's DPI setting matches the remote desktop's DPI setting, Display Scaling cannot take effect, even if you toggle the **Allow Display Scaling** option to on in the user interface. Windows does not allow users to change the system-level DPI setting for the current user session, and DPI synchronization occurs only when they log in and start a remote session. If users change the DPI setting during a remote session, they must log out and log in again to make the remote desktop's DPI setting match the client system's new DPI setting.

The agent DPI setting is located in the Windows registry at `Computer\HKEY_CURRENT_USER\Control Panel\Desktop:` *`logPixels`*.

Note The system DPI setting might not be the same as the main monitor's DPI setting. For example, if you close the main monitor and the system switches to an external display that has a different DPI setting than the main monitor, the system DPI setting is still the same as the DPI setting of the previously closed main monitor.

This version of Horizon Client does not support the **DPI Synchronization Per Connection** agent group policy setting, which is provided with Horizon Agent versions 7.8 through 2006.

For more information about the DPI synchronization group policy settings, see the *Configuring Remote Desktop Features in Horizon* document for your Horizon Agent version.

Supported Guest Operating Systems for Virtual Desktops

For virtual desktops, the DPI Synchronization feature is supported on the following guest operating systems:

- 32-bit or 64-bit Windows 7
- 32-bit or 64-bit Windows 8.x
- 32-bit or 64-bit Windows 10
- 32-bit or 64-bit Windows 11
- Windows Server 2008 R2 configured as a desktop
- Windows Server 2012 R2 configured as a desktop
- Windows Server 2016 configured as a desktop
- Windows Server 2019 configured as a desktop
- Windows Server 2022 configured as a desktop

Note For Windows server machines that are configured as a desktop, the DPI Synchronization Per Monitor feature is not supported.

Supported RDS Hosts for Published Desktops and Published Applications

For published desktops and published applications, the DPI Synchronization feature is supported on the following RDS hosts:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Note For RDS hosts, the DPI Synchronization Per Monitor feature is not supported. This limitation does not apply to published applications that run on desktop pools with the VM Hosted Applications feature.

Change the Display Mode for a Remote Desktop

You can change the display mode, such as from **Fullscreen - All Monitors** mode to **Fullscreen - Single Monitor** mode, before or after you connect to a remote desktop. This feature is not supported for published applications.

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box for the remote desktop.

- Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.
- Right-click the remote desktop in the desktop and application selection window and select **Settings**.

3 From the **Display** drop-down menu, select the display mode.

Option	Description
Fullscreen - All Monitors	Displays the remote desktop window on multiple monitors. The remote desktop window appears on all monitors by default.
Fullscreen - Single Monitor	Makes the remote desktop window fill the screen.
Window - Large	Maximizes the remote desktop window.
Window - Small	Sets the remote desktop window size to 640 x 480 pixels in 100 percent scaling.
Custom	Displays a slider that you can use to configure a custom remote desktop window size.

Results

If you are connected to the remote desktop, your changes are applied immediately. If you are not connected to the remote desktop, your changes are applied when you connect to it. Horizon Client saves display settings in a preferences file for the remote desktop after you exit from Horizon Client.

If you use **Fullscreen - All Monitors** mode and you click the **Minimize** button, if you then maximize the window, the window goes back to **Fullscreen - All Monitors** mode. Similarly, if you use **Fullscreen - Single Monitor** mode and minimize the window, if you then maximize the window, the window goes back to **Fullscreen - Single Monitor** mode on one monitor.

Note If Horizon Client uses all monitors, and you maximize a published application window, the window expands to the full screen of only the monitor that contains it.

Customize the Display Resolution and Display Scaling for a Remote Desktop

You can use Horizon Client to customize the display resolution and display scaling for a remote desktop. The display resolution determines the clarity of the text and images. At higher resolutions, such as 1600 x 1200 pixels, items appear sharper. Display scaling, which is represented as a percentage, increases or decreases the size of text, icons, and navigation elements.

By default, custom display resolution and display scaling settings are stored only on the local client system. An administrator can use the **Save resolution and DPI to server** group policy setting to save these settings to the server so that they are always applied, regardless of the client device that you use to log in to the remote desktop. For more information, see Using Group Policy Settings to Configure Horizon Client.

This feature has the following limitations and considerations.

- Customizing the display resolution and scaling for a remote desktop is not supported in multiple-monitor mode.
- If you select a custom resolution that is higher or lower than the client resolution, Horizon Client resizes the remote desktop window to fit the client window.
- If you customize the display resolution during a remote desktop session, your changes take effect immediately. If you customize display scaling during a remote desktop session, you must log out and log back in to make your changes take effect.
- The Horizon Client **Locked guest size** group policy setting takes precedence over display resolution customization. For more information, see Using Group Policy Settings to Configure Horizon Client.

Procedure

1. Start Horizon Client and connect to a server.
2. In the desktop and application selector window, right-click the remote desktop and select **Settings**.
3. From the **Connect Via** menu, select **VMware Blast** or **PCoIP**.
4. From the **Display** drop-down menu, select **Fullscreen - All Monitors**, **Fullscreen - Single Monitor**, **Window - Large**, **Window - Small**, or **Custom**.
5. To customize the display resolution, select a resolution from the **Resolution** drop-down menu.

   If you select **Automatic** (the default setting), Horizon Client fits the remote desktop to the client window size. If the remote desktop does not support the display resolution that you select, it uses the default setting.
6. To customize display scaling, select a scaling size from the **Scaling** drop-down menu.

   If you select **Automatic** (the default setting), Horizon Client synchronizes the client system's display scaling to the remote desktop.

Use USB Devices

With the USB redirection feature, you can use locally attached USB devices, such as thumb flash drives, in a remote desktop or published application.

When you use the USB redirection feature, most USB devices that are attached to the local client system become available from menus in Horizon Client. You use these menus to connect and disconnect the devices.

For information about USB device requirements and limitations for USB redirection, see the *Configuring Remote Desktop Features in Horizon* document.

You can connect USB devices to a remote desktop or published application either manually or automatically.

This procedure describes how to use Horizon Client to configure autoconnection of USB devices to a remote desktop or published application. You can also configure autoconnection by using the Horizon Client command-line interface, or by configuring a group policy.

For information about the command-line interface, see Running Horizon Client From the Command Line. For information about configuring group policies, see the *Configuring Remote Desktop Features in Horizon* document.

Prerequisites

- To use USB devices with a remote desktop or published application, a Horizon administrator must enable the USB redirection feature.

  This task includes installing the USB Redirection component of Horizon Agent, and can include setting policies regarding USB redirection. For more information, see the *Configuring Remote Desktop Features in Horizon* document and Using Group Policy Settings to Configure Horizon Client.

- The USB Redirection component must be installed in Horizon Client. If you did not include this component in the installation, uninstall Horizon Client and run the installer again to include the USB Redirection component.

  For installation instructions, see the *VMware Horizon Client for Windows Installation and Setup Guide* document.

- Become familiar with USB Redirection Limitations.

Procedure

- ◆ Manually connect the USB device to a remote desktop.

  a Connect the USB device to the local client system.

  b From the VMware Horizon Client menu bar in the remote desktop, click **USB Devices**.

  c Toggle the option for the USB device to on.

  The device is manually redirected from the local system to the remote desktop.

- ◆ Connect the USB device to a published application.

  a Connect the USB device to the local client system.

  b Start Horizon Client and connect to the published application.

  c Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selector window and click **USB Devices**.

   d In the right pane, select the published application and toggle the option for the USB device to on.

     Horizon Client connects the USB device to the published application that you selected. The USB device is also available to other applications in the same farm as the application that you selected.

   e (Optional) To configure Horizon Client to connect the USB device automatically to the published application when the application is started, select the **Automatically Connect at Startup** check box.

   f (Optional) To configure Horizon Client to connect the USB device automatically to the published application when you plug the device into the local system, select the **Automatically Connect when Inserted** check box.

     The published application must be activated and in the foreground for this behavior to take effect.

   g When you are finished using the published application, open the Settings dialog box again, select **USB Devices**, and toggle the option for the USB device to off.

     You must release the USB device so that you can access it from your local system.

- Configure Horizon Client to connect USB devices automatically to a remote desktop when you plug them in to the local system.

  Use the autoconnect feature if you plan to connect devices that use MTP drivers, such as Android-based Samsung smart phones and tablets.

  a Before you plug in the USB device, start Horizon Client and connect to the remote desktop.

  b From the VMware Horizon Client menu bar in the remote desktop, select **USB Devices > Automatically Connect when Inserted**.

  c Plug in the USB device.

  USB devices that you connect to your local system after you start Horizon Client are redirected to the remote desktop.

- Configure Horizon Client to connect USB devices automatically to a remote desktop when Horizon Client starts.

  a From the VMware Horizon Client menu bar in the remote desktop, select **USB Devices > Automatically Connect at Startup**.

  b Plug in the USB device and restart Horizon Client.

  USB devices that are connected to the local client system when you start Horizon Client are redirected to the remote desktop.

Results

The USB device appears in the remote desktop or published application. A USB device might take up to 20 seconds to appear in the remote desktop or published application. The first time you connect the device to a remote desktop you might be prompted to install drivers.

If the USB device does not appear in the remote desktop or published application after several minutes, disconnect and reconnect the device to the client computer.

What to do next

If you have problems with USB redirection, see the topic about troubleshooting USB redirection problems in the *Configuring Remote Desktop Features in Horizon* document.

USB Redirection Limitations

The USB redirection feature has certain limitations.

- When you access a USB device from a menu in Horizon Client and use the device in a remote desktop or published application, you cannot access the USB device on the local device.
- USB devices that do not appear in the menu, but are available in a remote desktop or published application, include human interface devices such as keyboards and pointing devices. The remote desktop or published application, and the local device, use these devices at the same time. Interaction with these USB devices can sometimes be slow because of network latency.
- Large USB disk drives can take several minutes to appear in the remote desktop or published application.
- Some USB devices require specific drivers. If a required driver is not already installed, you might be prompted to install it when you connect the USB device to the remote desktop or published application.
- If you plan to attach USB devices that use MTP drivers, such as Android-based Samsung smart phones and tablets, configure Horizon Client so that it connects USB devices to the remote desktop or published application automatically. Otherwise, if you try to manually redirect the USB device by using a menu item, the device is not redirected unless you unplug the device and then plug it in again.
- Do not connect to scanners by using the **USB Devices** menu. To use a scanner device, use the scanner redirection feature. See Using Scanners.
- The redirection of USB audio devices depends on the state of the network and is not reliable. Some devices require a high data throughput even when they are idle. Audio input and output devices work well with the Real-Time Audio-Video feature. You do not need to use USB redirection for those devices.
- You cannot format a redirected USB drive in a published desktop unless you connect as an administrator user.

- A published application auto-connects at startup and auto-connects when inserted features do not work with global application entitlements.
- The USB redirection feature does not support non-PCI USB controllers in the client system, such as the Fresco Logic F-One Controller. If you use such a controller in the client system, USB redirection might fail for all the USB devices in the client system.

Note Do not redirect USB devices such as USB Ethernet devices and touch screen devices to a remote desktop or published application. If you redirect a USB Ethernet device, your client system loses network connectivity. If you redirect a touch screen device, the remote desktop or published application receives touch input but not keyboard input. If you have set the remote desktop or published application to autoconnect USB devices, you can configure a policy to exclude specific devices.

Using Webcams and Microphones

With the Real-Time Audio-Video feature, you can use the local client system's webcam or microphone in a remote desktop or published application. Real-Time Audio-Video is compatible with standard conferencing applications and browser-based video applications. It supports standard webcams, audio USB devices, and analog audio input.

For information about setting up the Real-Time Audio-Video feature on the agent machine, including configuring the frame rate and image resolution, see the *Configuring Remote Desktop Features in Horizon* document.

When You Can Use a Webcam with the Real-Time Audio-Video Feature

If a Horizon administrator has configured the Real-Time Audio-Video feature, you can use a webcam that is built in or connected to the client computer in a remote desktop or published application. You can use the webcam in conferencing applications such as Skype, Webex, or Google Hangouts.

During the setup of an application such as Skype, Webex, or Google Hangouts on a remote desktop, you can select input and output devices from menus in the application.

For virtual desktops that have Horizon Agent 7.9 or earlier installed, and for published desktops and published applications, Real-Time Audio-Video can redirect only one webcam, and the webcam is named VMware Virtual Webcam in applications. For virtual desktops that have Horizon Agent 7.10 or later installed, Real-Time Audio-Video can redirect more than one webcam, and the redirected webcam name is the actual device name with (VDI) appended, for example, C670i FHD Webcam (VDI).

For many applications, you do not need to select an input device.

When the client computer uses the webcam, the remote session cannot use it at the same time. Also, when the remote session uses the webcam, the client computer cannot use it at the same time.

Important If you use a USB webcam, do not connect it from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and the performance is not usable for video chat.

If more than one webcam is connected to the client computer, you must configure a preferred webcam to use in remote sessions for published desktops and published applications, and for virtual desktops that do not support multiple webcams.

For more information, see Select a Preferred Webcam or Microphone on a Windows Client System.

Select a Preferred Webcam or Microphone on a Windows Client System

With the Real-Time Audio-Video feature, if multiple webcams or microphones are connected to the client system, you can specify which webcam or microphone is preferred by configuring Real-Time Audio-Video settings in Horizon Client.

With the Real-Time Audio-Video feature, video devices, audio input devices, and audio output devices work without requiring the use of USB redirection, and the amount of network bandwidth required is greatly reduced. Analog audio input devices are also supported.

If it is available, the preferred webcam or microphone is used in the remote desktop or published application. If the preferred webcam or microphone is not available, another webcam or microphone is used.

Note If you are using a USB webcam or microphone, do not connect it from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and the device cannot use the Real-Time Audio-Video feature.

For virtual desktops that have Horizon Agent 7.10 or later installed, the Real-Time Audio-Video feature supports multiple webcam and microphone devices.

Prerequisites

- Verify that a USB webcam or USB microphone, or other type of microphone, is installed and operational on the client system.
- Verify that you are using the VMware Blast display protocol or the PCoIP display protocol for the remote desktop or published application.
- Connect to a server.

Procedure

1 Open the **Settings** dialog box and select **Real-Time Audio-Video** in the left pane.

   - Click the **Settings** (gear) icon in the upper right corner of the desktop and application selector window.
   - Right-click a remote desktop or published application in the desktop and application selector window and select **Settings**.

2 To configure a preferred webcam, select a webcam from the **Preferred webcam** drop-down menu.

3 To configure a preferred microphone, select a specific microphone or **All** from the **Preferred microphone** drop-down menu.

   If the remote desktop supports multiple devices with the Real-Time Audio-Video feature and you select a specific microphone, only the selected microphone and webcam devices are redirected to the remote desktop. If you select **All**, all the available microphone and webcam devices are redirected to the remote desktop.

Using Multiple Devices with the Real-Time Audio-Video Feature

If more than one webcam or microphone is connected to the client computer, and the remote desktop supports multiple device redirection with the Real-Time Audio-Video feature, you can use all the webcams and microphones connected to the client computer in the remote desktop.

This feature is supported only with virtual desktops that have Horizon Agent 7.10 or later installed. It is not supported with published desktops or published applications. For complete system requirements, see System Requirements for Real-Time Audio-Video.

Following are tips for using more than one webcam or microphone with the Real-Time Audio-Video feature.

- When you connect to a remote desktop, the Real-Time Audio-Video feature redirects all webcams and microphones currently connected to the client computer. The remote desktop decides which webcam and microphone is the default device. You do not need to configure a preferred webcam or microphone in Horizon Client.
- If you want to use the same microphone by default in applications such as Skype for Business, you must configure a default microphone. Otherwise, all microphones are redirected and you must select a microphone each time you use the application. For more information, see Select a Preferred Webcam or Microphone on a Windows Client System.
- If you disconnect a webcam or microphone from the client computer, and the device is not being used in an application in the remote desktop, the Real-Time Audio-Video feature deletes the device in the remote desktop immediately. If the device is being used by an application in the remote desktop, the Real-Time Audio-Video feature deletes the device after the application releases it.

- The display name of a redirected device is the actual device name, but with (VDI) appended, for example, C670i FHD Webcam (VDI).
- You can use multiple redirected devices simultaneously in a remote desktop.

Select a Preferred Speaker for a Remote Desktop

If multiple speakers are connected to the client system, you can specify which speaker is preferred in a remote desktop. You can also select all the available speakers.

This feature is supported only with virtual desktops. It is not supported with published desktops and published applications.

If you select a specific speaker and then add or remove a speaker from the client system during a remote session, the changes do not take effect in the remote session. If you select all the available speakers, the devices are updated dynamically during a remote session.

Prerequisites

- Verify that multiple speakers are installed and operational on the client system.
- Verify that you are using the VMware Blast display protocol to connect to the remote desktop. This feature does not work with any other display protocols.
- Verify that Horizon Agent 2012 or later is installed in the remote desktop. For earlier Horizon Agent versions, audio is played back on the default audio device attached to the client system.
- Connect to the server.

Procedure

1 Open the **Settings** dialog box and select **Real-Time Audio-Video** in the left pane.

   - Click the **Settings** (gear) icon in the upper right corner of the desktop and application selector window.
   - Right-click the remote desktop in the desktop and application selector window and select **Settings**.

2 Select a speaker from the **Preferred speaker** drop-down menu.

   Note This feature is independent of the Real-Time Audio-Video feature, even though it appears on the**Real-Time Audio-Video** page.

   If you select a specific speaker, only the selected speaker is redirected to the remote desktop. If you select **All**, all the available speakers are redirected to the remote desktop. If you select **Default**, audio is played back on the default audio device attached to the client system.

Sharing Remote Desktop Sessions

With the Session Collaboration feature, you can invite other users to join an existing remote desktop session. A remote desktop session that is shared in this way is called a collaborative session. The user that shares a session with another user is called the session owner, and the user that joins a shared session is called a session collaborator.

A Horizon administrator must enable the Session Collaboration feature.

For Windows desktops, this task includes enabling the Session Collaboration feature at the desktop pool or farm level. It can also include using group policies to configure Session Collaboration features, such as the available invitation methods. For complete requirements, see System Requirements for the Session Collaboration Feature.

For information about enabling the Session Collaboration feature for Windows desktops, see the *Setting Up Virtual Desktops in Horizon* document. For information about enabling the Session Collaboration feature for a farm, see the *Setting Up Published Desktops and Applications in Horizon* document. For information about using group policy settings to configure the Session Collaboration feature, see the *Configuring Remote Desktop Features in Horizon* document.

For information about enabling the Session Collaboration feature for Linux desktops, see the *Setting Up Linux Desktops in Horizon* document.

Invite a User to Join a Remote Desktop Session

With the Session Collaboration feature, you can invite users to join a remote desktop session by sending collaboration invitations by email, in an instant message (Windows remote desktops only), or by copying a link to the clipboard and forwarding the link to users.

You can invite only users that belong to a domain that the server allows for authentication. You can invite up to five users by default. A Horizon administrator can change the maximum number of users that you can invite.

The Session Collaboration feature has the following limitations.

- If you have multiple monitors, only the primary monitor is shown to session collaborators.
- You must select the VMware Blast display protocol when you create a remote desktop session to share. The Session Collaboration feature does not support PCoIP or RDP sessions.
- H.264 hardware encoding is not supported. If the session owner is using hardware encoding and a collaborator joins the session, both fall back to software encoding.
- Anonymous collaboration is not supported. Session collaborators must be identifiable through Horizon-supported authentication mechanisms.
- Session collaborators must have Horizon Client for Windows, Mac, or Linux installed, or they must use HTML Access.
- If a session collaborator has an unsupported version of Horizon Client, an error message appears when the user clicks a collaboration link.
- You cannot use the Session Collaboration feature to share published application sessions.

Prerequisites

- The Session Collaboration feature must be enabled and configured.

- To use the email invitation method, an email application must be installed.
- To use the IM invitation method for a Windows remote desktop, Skype for Business must be installed and configured.

Procedure

1 Connect to a remote desktop for which the Session Collaboration feature is enabled.

You must use the VMware Blast display protocol.

2 In the system tray in the remote desktop, click the **VMware Horizon Collaboration** icon, for example, .

The collaboration icon might look different, depending on the operating system version.

3 When the VMware Horizon Collaboration dialog box opens, enter the user name (for example, **`testuser`** or **`domain\testuser`**) or the email address of the user that you want to join the remote desktop session.

The first time you enter the user name or email address of a particular user, you must click **Look up "*user*"**, enter a comma (,), or press the **Enter** key to validate the user. For Windows remote desktops, the Session Collaboration feature remembers the user the next time you enter the user's user name or email address.

4 Select an invitation method.

Not all invitation methods might be available.

Option	Action
Email	Copies the collaboration invitation to the clipboard and opens a new email message in the default email application. An email application must be installed to use this invitation method.
IM	(Windows remote desktops only) Copies the collaboration invitation to the clipboard and opens a new window in Skype for Business. Press Ctrl+V to paste the link into the Skype for Business window. Skype for Business must be installed and configured to use this invitation method.
Copy Link	Copies the collaboration invitation to the clipboard. You must manually open another application, such as Notepad, and press Ctrl+V to paste the invitation.

Results

After you send an invitation, the VMware Horizon Collaboration icon also appears on the desktop and the Session Collaboration user interface turns into a dashboard that shows the current state of the collaboration session and enables you to take certain actions.

When a session collaborator accepts your invitation to join a Windows remote desktop session, the Session Collaboration feature notifies you and a red dot appears on the VMware Horizon Collaboration icon in the system tray. When a session collaborator accepts your invitation to join a Linux remote desktop session, a notification appears in the primary session desktop.

What to do next

Manage the remote desktop session in the VMware Horizon Collaboration dialog box. See Manage a Shared Remote Desktop Session.

Manage a Shared Remote Desktop Session

After you send a session collaboration invitation, the Session Collaboration user interface turns into a dashboard that shows the current state of the shared remote desktop session (collaborative session) and enables you to take certain actions.

A Horizon administrator can prevent the hand off of control to a session collaborator. For Windows remote desktops, see the **Allow control passing to collaborators** group policy setting in the *Configuring Remote Desktop Features in Horizon* document. For Linux remote desktops, see the `collaboration.enableControlPassing` parameter in the *Setting Up Linux Desktops in Horizon* document.

Prerequisites

Start a collaborative session. See Invite a User to Join a Remote Desktop Session.

Procedure

1 In the remote desktop, click the **VMware Horizon Collaboration** icon in the system tray.

The names of all session collaborators appear in the Name column and their status appears in the Status column.

2 Use the VMware Horizon Session Collaboration dashboard to manage the collaborative session.

Option	Action
Revoke an invitation or remove a collaborator	Click **Remove** in the Status column.
Hand off control to a session collaborator	After the session collaborator joins the session, toggle the switch in the Control column to **On**. To resume control of the session, double-click or press any key. The session collaborator can also give back control by toggling the switch in the Control column to **Off**, or by clicking the **Give Back Control** button.
Add a collaborator	Click **Add Collaborators**.
End the collaborative session	Click **End Collaboration**. All active collaborators are disconnected. In Windows remote desktops, you can also end the collaborative session by clicking the **Stop** button next to the **VMware Horizon Session Collaboration** icon. The **Stop** button is not available in Linux remote desktops.

Join a Remote Desktop Session

With the Session Collaboration feature, you can click the link in a collaboration invitation to join a remote desktop session. The link might be in an email or instant message, or in a document that the session owner forwards to you. Alternatively, you can log in to the server and double-click the icon for the session in the remote desktop and application selector window.

This procedure describes how to join a remote desktop session from a collaboration invitation.

Note In a Cloud Pod Architecture environment, you cannot join a collaborative session by logging in to the server unless you log in to the session owner's pod.

When you join a remote desktop session with the Session Collaboration feature, you cannot use the following features in the remote desktop session.

- USB redirection
- Real-Time Audio-Video (RTAV)
- Multimedia redirection
- Client drive redirection
- Smart card redirection
- VMware Integrated Printing
- Microsoft Lync redirection
- File redirection and Keep in Dock functionality
- Clipboard redirection

You also cannot change the remote desktop resolution in the remote desktop session.

Prerequisites

To join a remote desktop session with the Session Collaboration feature, you must have Horizon Client for Windows, Mac, or Linux installed on the client system, or you must use HTML Access.

Procedure

1 Click the link in the collaboration invitation.

  Horizon Client opens on the client system.

2 Enter your credentials to log in to Horizon Client.

  After you are successfully authenticated, the collaborative session begins and you can see the session owner's remote desktop. If the session owner transfers mouse and keyboard control to you, you can use the remote desktop.

3 To return mouse and keyboard control to the session owner, click the **VMware Horizon Collaboration** icon in the system tray and toggle the switch in the Control column to **Off**, or click the **Give Back Control** button.

4 To leave the collaborative session, click **Options > Disconnect**.

Share Local Folders and Drives

With the client drive redirection feature, you can share folders and drives on the local client system with remote desktops and published applications.

Shared drives can include mapped drives and USB storage devices. Mapped drives can have UNC (Universal Naming Convention) paths.

The maximum length of a shared folder name is 117 characters.

The client drive redirection feature does not support sharing Microsoft OneDrive, Google Drive, and enterprise file storage.

In a Windows remote desktop, shared folders and drives appear in the **This PC** folder or in the **Computer** folder, depending on the Windows operating system version. In a published application, such as Notepad, you can browse to and open a file in a shared folder or drive.

The client drive redirection settings apply to all remote desktops and published applications.

Prerequisites

To share folders and drives with a remote desktop or published application, the client drive redirection feature must be installed in Horizon Agent. The client drive redirection feature is installed by default.

You can hide the client drive redirection feature in Horizon Client by enabling a group policy setting. For more information, see **Disable sharing files and folders** in Using Group Policy Settings to Configure Horizon Client.

With Horizon Agent 7.8 and later, you can configure drive letter behavior for drives that are redirected by the client drive redirection feature by configuring the **Display redirected device with drive letter** group policy setting. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

With Horizon Agent 7.9 and later, you can include or exclude folders on devices that have specified vendor and product IDs from being redirected by using the **Include Vid/Pid Device** and **Exclude Vid/Pid Device** group policy settings. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

With Horizon Agent 7.10 and later, you can configure how drive letters are mapped by using the **Configure drive letter mapping mode** and **Define drive letter mapping table** group policy settings. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

If the secure tunnel is enabled on the Connection Server instance, configuring the browser on the client system to use a proxy server can cause poor client drive redirection performance. For the best client drive redirection performance, configure the browser not to use a proxy server or detect LAN settings automatically.

Procedure

1 Open the Settings dialog box and display the Drive Sharing panel.

Option	Description
From the desktop and application selector window	Right-click a remote desktop or published application icon, select **Settings**, and select **Drive Sharing** in the left panel of the window that appears.
From the Sharing dialog box that appears when you connect to a remote desktop or published application	Click the **Settings > Drive Sharing** link in the dialog box.
From within a remote desktop	Select **Options > Settings > Drive Sharing** from the menu bar.

2 Configure the client drive redirection settings.

Option	Action
Share a specific folder or drive with remote desktops and published applications	Click the **Add** button and browse to and select the folder or drive to share. **Note** If a USB device is already connected to a remote desktop or published application with the USB redirection feature, you cannot share a folder on the USB device. Also, do not turn on the USB redirection feature that connects USB devices automatically at startup or when the device is inserted. If you do so, the next time you start Horizon Client or plug in the USB device, the device connects with the USB redirection feature instead of with the client drive redirection feature. If drive letter mapping is configured, the folders configured in the share list are not redirected. For more information, see "Use Group Policy to Configure Drive Letter Behavior" in the *Configuring Remote Desktop Features in Horizon* document.
Stop sharing a specific folder or drive	Select the folder or drive in the Folder list and click the **Remove** button.
Give remote desktops and published applications access to files in your local user directory	Toggle the **Share your local files** ***user-name*** option to on.

Option	Action
Share USB storage devices with remote desktops and published applications	Toggle the **Allow auto access to removable storage** option to on. The client drive redirection feature shares all USB storage devices inserted in your client system and all FireWire and Thunderbolt-connected external drives automatically. Selecting a specific device to share is not necessary. **Note** USB storage devices already connected to a remote desktop or published application with the USB redirection feature are not shared. If you are using an encrypted USB thumb drive, you must start Horizon Client before you plug in the USB device so that Horizon Client can detect the device. If this option is toggled off, you can use the USB redirection feature to connect USB storage devices to remote desktops and published applications.
Do not show the Sharing dialog box when you connect to a remote desktop or published application	Select the **Do not show dialog when connecting to a desktop or application** check box. If this check box is deselected, the Sharing dialog box appears the first time you connect to a remote desktop or published application. For example, if you log in to a server and connect to a remote desktop, you see the Sharing dialog box. If you then connect to another remote desktop or published application, you do not see the dialog box. To see the dialog box again, you must disconnect from the server and log in again.

What to do next

Verify that you can see the shared folders from within the remote desktop or published application.

- In a Windows remote desktop, open File Explorer and look in the **This PC** folder, or open Windows Explorer and look in the **Computer** folder, depending on the Windows operating system version.
- In a published application, select **File > Open** or **File > Save As** and navigate to the folder or drive.

The folders and drives that you selected for sharing might use one (or more) of the following naming conventions.

Naming Convention	Example
folder-name on *desktop-name*	jsmith on JSMITH-W03
folder-name (*drive-number*:)	jsmith (Z:)
folder-name on *desktoptop-name* (*drive-number*:)	jsmith on JSMITH-W03 (Z:)

For some Horizon Agent versions, a redirected folder can have two entrances, such as under **Devices and drives** and **Network locations** in Windows 10, and both entrances can appear at the same time. If all the volume labels (from A: through Z:) are already in use, the redirected folder has only one entrance.

Open Local Files in Published Applications

You can turn on the ability to open local files in published applications directly from the local file system.

With this feature, the **Open with** menu on the client system lists the available published applications when you right-click a local file.

You can also set files to be opened automatically in published applications when you double-click the file. With this feature, all files on your local file system that have certain file extensions are registered with the server that you are logged in to. For example, if Microsoft Word is a published application on the server, you can right-click a `.docx` file on your local file system and open the file with the Microsoft Word published application.

Prerequisites

To open local files in published applications, a Horizon administrator must install the client drive redirection feature in Horizon Agent. The client drive redirection feature is installed by default. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

You can hide the client drive redirection feature in Horizon Client by enabling a group policy setting. For more information, see **Disable sharing files and folders** in Using Group Policy Settings to Configure Horizon Client.

Procedure

1 Connect to a server.

2 Open the Settings dialog box and display the Applications panel.

Option	Description
From the desktop and application selector window	Right-click a remote desktop or published application icon, select **Settings**, and select **Applications** in the left panel of the window that appears.
From the system tray icon context menu when you connect to a remote desktop or published application	Click the **Settings > Sharing** link in the dialog box.
From within a remote desktop	Select **Options > Settings** from the menu bar in the remote desktop and select **Applications** in the left panel of the window that appears.

3 Select the **Open local files in hosted applications** check box.

When this option is enabled, you can right-click a file in your local file system and select to open the file in a published application. You can also change the properties of the file so that all files with that file extension are opened with the published application by default, such as when you double-click the file. For example, you can right-click a file, select **Properties**, and click **Change** to select the published application to open files of that type.

Copying and Pasting

By default, you can copy and paste from the client system to a remote desktop or published application.

If you use the VMware Blast display protocol or the PCoIP display protocol, a Horizon administrator can configure this feature so that copy and paste operations are allowed only from the client system to a remote desktop or published application, or only from a remote desktop or published application to the client system, or both, or neither.

The following data formats are supported.

- CF_BITMAP
- CF_DIB
- CF_HDROP (file type)
- CF_UNICODETEXT
- Biff12
- Art::GVML ClipFormat
- HTML Format
- RTF (Rich Text Format)

A Horizon administrator configures the ability to copy and paste by setting agent group policies. Depending on the Horizon server and agent version, a Horizon administrator might also be able to use group policies to restrict clipboard formats during copy and paste operations, or use Smart Policies to control the copy and paste behavior in remote desktops. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Copying and Pasting Text and Images

By default, you can copy and paste from the client system to a remote desktop or published application. You can also copy and paste from a remote desktop or published application to the client system, or between two remote desktops or published applications, if a Horizon administrator enables these features.

For example, to copy text on the client system, select the text and press Ctrl+C. To paste the text into a remote desktop, press Ctrl+V in the remote desktop.

This feature has the following limitations.

- If you are copying formatted text, some of the data is text and some of the data is formatting information. If you copy a large amount of formatted text or text and an image, when you attempt to paste the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.

- If the text and RTF data together use less than the maximum clipboard size, the formatted text is pasted. Often, the RTF data cannot be truncated, so that if the text and formatting use more than the maximum clipboard size amount, the RTF data is discarded, and the plain text is pasted.
- If you are unable to paste all the formatted text and images that you selected in one operation, you might need to copy and paste smaller amounts in each operation.

Copying and Pasting Files and Folders

By default, you can copy and paste files and folders from your client system to a remote desktop or published application. You can also copy and paste files and folders from a remote desktop or published application to the client system if a Horizon administrator enables these features.

For example, to copy a file on the client system, select the file and press Ctrl+C. To paste the file into a remote desktop, press Ctrl+V in the remote desktop.

This feature requires Horizon Agent 2012 or later on the agent machine.

The client drive redirection feature must be installed on the agent machine to use this feature. For more information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

You can disable this feature by enabling the **Filter files and folders from incoming clipboard data** and **Filter files and folders from outgoing clipboard data** settings in the **Configure clipboard redirection formats** group policy setting for the agent machine. For information about the agent group policy settings that control this feature, see the *Configuring Remote Desktop Features in Horizon* document.

This feature has the following limitations.

- It might not work for some special folders, such as the desktop folder or a recently accessed file list folder, when you try to copy and paste multiple files because the folder might show files and folders that are not in the same parent folder. This feature can only copy and paste files and folders that are in the same parent folder.
- It might not work for certain applications, such as WordPad and PowerPoint.
- Only one copy and paste operation is allowed at a time. Additional copy and paste operations are ignored.

Logging Copy and Paste Activity

When you enable the clipboard audit feature, Horizon Agent records information about copy and paste activity in an event log on the agent machine. The clipboard audit feature is disabled by default.

This feature applies only to copying and pasting text and images. It does not apply to copying and pasting files and folders.

To enable the clipboard audit feature, you must configure the **Configure clipboard audit** group policy setting.

If Horizon Agent 7.6 is installed on the agent machine, only information about clipboard data that is copied from the agent machine to the client machine is recorded in the event log. If Horizon Agent 7.7 or later is installed on the agent machine, you can configure the clipboard audit feature to record information only about data that is copied from the client machine to the agent machine, only about data that is copied from the agent machine to the client machine, or about data that are copied in both directions.

You can optionally configure the **Whether block clipboard redirection to client side when client doesn't support audit** group policy setting to specify whether to block clipboard redirection to clients that do not support the clipboard audit feature.

For more information about the group policy settings for clipboard redirection, see the *Configuring Remote Desktop Features in Horizon* document.

The event log where information about copy and paste activity is recorded is named VMware Horizon RX Audit. To view the event log on the agent machine, use the Windows event viewer. To view the event log from a centralized location, configure VMware Log Insight or Windows Event Collector. For information about Log Insight, go to https://docs.vmware.com/en/vRealize-Log-Insight/index.html. For information about Windows Event Collector, see the Microsoft documentation.

Configuring the Client Clipboard Memory Size

The clipboard memory size is configurable for both the server and the client.

This feature applies only to copying and pasting text and images. It does not apply to copying and pasting files and folders.

When a PCoIP or VMware Blast session is established, the server sends its clipboard memory size to the client. The effective clipboard memory size is the lesser of the server and client clipboard memory size values.

To set the client clipboard memory size, modify the Windows registry value `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. The value type is REG_DWORD. The value is specified in KB. If you specify 0 or do not specify a value, the default client clipboard memory size is 8192 KB (8 MB).

A large clipboard memory size can negatively affect performance, depending on your network. VMware recommends that you do not set the clipboard memory size to a value greater than 16 MB.

To transfer larger amounts of data, use the client drive redirection feature.

Dragging and Dropping

The drag and drop feature works differently depending on the Horizon Agent version and how it is configured.

With Horizon Agent 7.9 and later, you can drag and drop files, folders, text, rich text, and images between the client system and remote desktops and published applications. With Horizon Agent 7.7 and 7.8, you can drag and drop only files and folders between the client system and remote desktops and published applications. Earlier Horizon Agent versions do not support drag and drop.

The following data formats are supported.

- HTML Format
- Rich Text Format (RTF)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor
- FileContents

Depending on the Horizon Agent version, a Horizon administrator can use certain group policy settings or Smart Policies to configure drag and drop behavior. For complete information about configuring the drag and drop feature, see the *Configuring Remote Desktop Features in Horizon* document for your VMware Horizon version.

Dragging Text and Images

With Horizon Agent 7.9 and later, you can drag text, images, and other data formats from the client system to an open application in a remote desktop or a published application. For example, you can drag text from a browser on the client system and drop it into the WordPad application in a remote desktop. Depending on how the drag and drop feature is configured, you might also be able to drag text, images, and other data formats from an open application in a remote desktop or a published application to the client system.

A Horizon administrator can configure drag and drop behavior by configuring group policy settings. With Horizon Agent 7.9 and Dynamic Environment Manager 9.8 and later, a Horizon administrator can also use Smart Policies to configure drag and drop behavior, including disabling the entire drag and drop feature. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Dragging Files and Folders

With Horizon Agent 7.7 and later, you can drag and drop files and folders between the Windows client system and remote desktops and published applications. You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.

If you drag a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.

By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled. A Horizon administrator can control the drag and drop direction by configuring group policy settings.

Dragging and dropping files, folders, and file contents requires that the client drive redirection feature is installed in Horizon Agent. The client drive redirection feature is installed by default. For complete information about configuring the drag and drop feature, including feature requirements, see the *Configuring Remote Desktop Features in Horizon* document for your VMware Horizon version.

Tips for Using the Drag and Drop Feature

When using the drag and drop feature, follow these tips.

Note Depending on the Horizon Agent version, some tips might not apply to your environment.

- You must use the VMware Blast or PCoIP display protocol.
- If the relative mouse feature is enabled (select **Settings > Enable Relative Mouse** after you connect to a remote desktop that supports this feature), you can drag and drop only from the client system to a virtual desktop.
- When a drag and drop operation is in progress, you cannot start a new drag and drop operation until after the first drag and drop operation has finished.
- You cannot use the drag and drop feature in nested mode.
- When dragging and dropping, you must use the primary mouse button (by default the left button). Using the secondary mouse button (by default the right button), and pressing Ctrl+Shift+Alt plus the primary mouse button, are not supported.
- You cannot drag and drop between remote desktops.
- You cannot drag and drop between published applications from different farms.
- If you drag and drop a file or folder between the client system and a remote desktop, the file or folder appears in the file system on the target system. If you drag a file and drop it into an open application, such as Notepad, the text appears in the application. If you drag a file into a new email message, the file becomes an attachment to the email message.

- You can drag and drop multiple files and folders at the same time. A progress bar shows the status of the drag and drop operation.
- By default, dragging and dropping from the client system to remote desktops and published applications is enabled, and dragging and dropping from remote desktops and published applications to the client system is disabled.
- If you are dragging formatted text, some of the data is text and some of the data is formatting information. If you drag a large amount of formatted text, or text and an image, when you attempt to drop the text and image, you might see some or all the plain text, but no formatting or image. This problem occurs because the three types of data are sometimes stored separately. For example, depending on the type of document, images might be stored as images or as RTF data.
- If you are dragging both plain text and RTF data, and the total data size is less than the drag and drop size threshold, the formatted text is copied. Because RTF data cannot be truncated, if the total data size is greater than the drag and drop size threshold, the RTF data is discarded and only the plain text (or part of the plain text) is copied.
- If you are unable to drag all the formatted text and images in one operation, you might need to drag smaller amounts in each operation.
- When you drag a file from the client system and drop it into a published application, you cannot click **Save as** to copy the file back to a different file on the client system. You can click **Save** to copy the file back to the same file on the client system.
- If you drag a file from the client system to an application in a remote desktop, the file is copied to the remote desktop and you can only edit the copy of the file.
- In a 64-bit Windows machine, if you are unable to drag from Horizon Client to a local 64-bit application, try using the 32-bit version of the local application.
- If the target local application fails to accept the dragged object, try dragging the object to the local file system and then dragging it to the target local application from local file system.
- A built-in timeout mechanism exists for fault tolerance.

Tips for Using Published Applications

Published applications look and feel like applications that are installed on the local client system. When using published applications, follow these tips.

- You can minimize and maximize a published application through the published application. When a published application is minimized, it appears in the taskbar of the client system. You can also minimize and maximize the published application by clicking its icon in the taskbar.
- You can quit a published application through the published application or by right-clicking its icon in the taskbar.
- You can press Alt+Tab to switch between open published applications.

- If a published application creates a Windows System Tray item, that item also appears in the system tray on the client system. By default, the system tray icons appear only to show notifications. You can customize this behavior in the same way that you customize natively installed applications.

  Note If you open the Control Panel to customize the notification area icons, the names of the icons for published applications are listed as VMware Horizon Client - *application name*.

Reconnect to Published Applications After Disconnecting

Running published applications can remain open after you disconnect for a server in Horizon Client. You can configure how running published applications behave when you reconnect to the server in Horizon Client.

You can disable the published application reconnection behavior settings in Horizon Client, either from the command line, or by configuring a group policy setting. The group policy setting takes precedence over the command-line setting. For more information, see the `-appSessionReconnectionBehavior` option in Install Horizon Client From the Command Line, or the **Disconnected application session resumption behavior** group policy setting in Using Group Policy Settings to Configure Horizon Client.

Procedure

1. In the Horizon Client desktop and application selector window, right-click a published application and select **Settings**.
2. In the Applications pane, select an application reconnection behavior setting.

Option	Description
Ask to reconnect to open applications	Horizon Client notifies you that you have one or more published applications running when you reconnect to the server. You can click **Open applications** to reopen the published application windows, or **Not now** not to reopen the published application windows.
Reconnect automatically to open applications	Windows for running published applications reopen when you reconnect to the server.
Do not ask and do not automatically reconnect	Horizon Client does not prompt you to reopen running published applications, and running published application windows do not reopen when you reconnect to the server.

Results

The setting takes effect the next time Horizon Client connects to the server.

Use Multiple Sessions of a Published Application From Different Client Devices

When multi-session mode is enabled for a published application, you can use multiple sessions of the same published application when you log on to the server from different client devices.

For example, if you open a published application in multi-session mode on client A, and then open the same published application on client B, the published application remains open on client A and a new session of the published application opens on client B. By comparison, when multi-session mode is disabled (single-session mode), the published application session on client A disconnects and reconnects on client B.

The multi-session mode feature has the following limitations.

- Multi-session mode does not work for applications that do not support multiple instances, such as Skype for Business.
- If the application session is disconnected while you are using a published application in multi-session mode, you are logged off automatically and any unsaved data is lost.

Prerequisites

A Horizon administrator must enable multi-session mode for the application pool. Users cannot modify the multi-session mode for a published application unless a Horizon administrator allows it. See *Setting Up Published Desktops and Applications in Horizon*. This feature requires Horizon 7 version 7.7 or later.

Procedure

1. Connect to a server.
2. Open the Settings dialog box and select **Multi-Launch** in the left pane.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window.
   - Right-click a remote desktop or published application in the desktop and application selection window and select **Settings**.

   If no published applications are available to use in multi-session mode, the **Multi-Launch** setting does not appear.
3. Select the published applications that you want to use in multi-session mode and toggle the **Multi-Launch** option to on or off.

   If a Horizon administrator has enforced multi-session mode for a published application, you cannot change this setting.

Use a Local IME with Published Applications

If you use non-English keyboards and locales, you can use an IME (input method editor) that is installed in the local client system to send non-English characters to published applications.

You can use hot keys and icons in the notification area (system tray) of the local client system to switch to a different IME. You do not need to install an IME on the server that hosts the published application.

When this feature is enabled, the local IME is used. If an IME is installed and configured on the server that hosts the published application, that remote IME is ignored.

This feature is disabled by default. When you enable or disable this feature, you must disconnect from the server and log in again before the change takes effect.

Prerequisites

- Verify that one or more IMEs are installed in the client system.
- Verify that the input language on the local client system matches the language used in the IME.

Procedure

1. Start Horizon Client and connect to a server.
2. In the desktop and application selector window, right-click a published application and select **Settings**.
3. In the **Applications** pane, toggle the **Extend the local IME to hosted applications** option to on.
4. Restart the session.

Option	Action
Log off of the server	Disconnect from the server, log in again, and reconnect to the published application. You can resume the published applications, which were disconnected but not closed, and any remote desktops.
Reset the applications	Right-click a published application, select **Settings**, and click **Reset**. When you use this option, any open remote desktops are not disconnected, but all published applications are closed and must be restarted.

   The setting takes effect only after you restart the session. The setting applies to all published applications on the server.

5. Use the local IME as you might use it with locally installed applications.

Results

The language designation and an icon for the IME appear in the notification area (system tray) of the local client system. You can use hot keys to switch to a different language or IME. Key combinations that perform certain actions, such as CTRL+X for cutting text and Alt+Right Arrow for moving to a different tab, work correctly.

Note On Windows 8.x systems, you can specify hot keys for IMEs by using the **Text Services and Input Languages** dialog box, which is available at **Control Panel > Region and Language > Keyboards and Languages tab > Change Keyboards button > Text Services and Input Languages > Advanced Key Settings tab**).

Use a Local IME with a Remote Desktop

If you use non-English keyboards and locales, you can use an IME (input method editor) that is installed in the local client system to send non-English characters to a remote desktop. Horizon Client supports Simplified Chinese, Traditional Chinese, Japanese and Korean. Right-click options are supported for Japanese and Korean.

This feature is disabled by default. When this feature is enabled, you can use hot keys and icons in the notification area (system tray) of the local client system to switch to a different IME.

Prerequisites

- Verify that one or more IMEs are installed in the client system.

  You do not need to install an IME on the remote desktop. If an IME is installed and configured on the remote desktop, it is ignored.

- Verify that the input language on the local client system matches the language used in the IME.

Procedure

1. Start Horizon Client and connect to a server.
2. Open the **Settings** dialog box for the remote desktop.
   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.
   - Right-click the remote desktop in the desktop and application selection window and select **Settings**.
3. Select **Extend the local IME to this desktop**.
4. Start the remote desktop and use the local IME as you might use it with locally installed applications.

Results

A new VMware IME is activated on the remote desktop automatically, and the IME conversion status is synchronized in each direction between the local client system and the remote desktop.

The language designation and an icon for the IME appear in the notification area (system tray) of the local client system. You can use hot keys to switch to a different language or IME. Key combinations that perform certain actions, such as CTRL+X for cutting text and Alt+Right Arrow for moving to a different tab, work correctly.

Note On Windows 8.x systems, you can specify hot keys for IMEs by using the **Text Services and Input Languages** dialog box, which is available at **Control Panel > Region and Language > Keyboards and Languages tab > Change Keyboards button > Text Services and Input Languages > Advanced Key Settings tab**).

Printing From a Remote Desktop or Published Application

With the VMware Integrated Printing feature, you can print to a network printer or a locally attached printer from a remote desktop or published application.

For information about installing the VMware Integrated Printing feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

For information about configuring the VMware Integrated Printing feature, see the *Configuring Remote Desktop Features in Horizon* document.

For information about the types of remote desktops that support the VMware Integrated Printing feature, see Feature Support for Windows Clients.

Set Printing Preferences for the VMware Integrated Printing Feature

You can set printing preferences in a remote desktop for the VMware Integrated Printing feature. With the VMware Integrated Printing feature, you can use local or network printers from a remote desktop without having to install additional printer drivers in the Windows remote desktop. For each printer available through this feature, you can set preferences for data compression, print quality, double-sided printing, color, and other settings.

In a single-user virtual machine desktop, each virtual printer appears as *<printer_name>*(*vdi*) by default. In a published desktop or published application, each virtual printer appears as *<printer_name>*(v*<session_ID>*) by default.

Beginning with Horizon Agent 7.12, you can use group policy to modify the printer naming convention for client printers that are redirected. For information, see the *Configuring Remote Desktop Features in Horizon* document for your Horizon Agent version.

You can use the Windows Registry to configure default VMware Integrated Printing settings for Horizon Client. See Using the Windows Registry to Configure Horizon Client.

Prerequisites

To use VMware Integrated Printing, a Horizon administrator must install the VMware Integrated Printing feature in the remote desktop. This task involves enabling the **VMware Integrated Printing** option in the Horizon Agent installer. For information about installing Horizon Agent, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document. For information about configuring the VMware Integrated Printing feature, see the *Configuring Remote Desktop Features in Horizon* document.

To determine whether the VMware Integrated Printing feature is installed in a remote desktop, verify that the `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-server.exe` and `C:\Program Files\Common Files\VMware\Remote Experience\x64\vmware-print-redir-service.exe` files exist in the remote desktop file system.

This feature requires Horizon Agent 7.7 or later.

Procedure

1. In the Windows remote desktop, go to **Control Panel > Hardware and Sound > Devices and Printers**.
2. In the **Devices and Printers** window, right-click the virtual printer and select **Printer properties** from the context menu.
3. On the **General** tab, click **Preferences**.
4. In the Printing Preferences dialog box, select the different tabs and specify which settings to use.
5. To save your changes, click **OK**.

Printing From a Remote Desktop to a Local USB Printer

A USB printer is a printer that is attached to a USB port on the local client system. You can send print jobs to a USB printer attached to the local client system from a remote desktop.

You can use either the USB redirection feature or the VMware Integrated Printing feature to print to a USB printer from a remote desktop. Redirected USB printers and virtual printers can work together without conflict.

Using the USB Redirection Feature

To use the USB redirection feature to attach a USB printer to a virtual USB port in a remote desktop, the required printer drivers must be installed in the remote desktop as well as on the client system.

When you use the USB redirection feature to redirect a USB printer, the USB printer is no longer logically attached to the physical USB port on the local client system and it does not appear in the list of local printers on the local client system. You can print to the USB printer from the remote desktop, but you can no longer print to the USB printer from the local client system.

In a remote desktop, redirected USB printers appear as *<printer_name>*.

Using the VMware Integrated Printing Feature

When you use the VMware Integrated Printing feature to send print jobs to a USB printer, you can print to the USB printer from both the remote desktop and the local client system and you do not need to install printer drivers in the remote desktop.

To use the VMware Integrated Printing feature, the feature must be enabled when you install Horizon Agent. For installation information, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

For more information, see Set Printing Preferences for the VMware Integrated Printing Feature.

Improve Mouse Performance in a Remote Desktop

If you use the VMware Blast display protocol or the PCoIP display protocol when using 3D applications in a remote desktop, mouse performance improves when you enable the relative mouse feature.

In most circumstances, if you are using applications that do not require 3D rendering, Horizon Client transmits information about mouse pointer movements by using absolute coordinates. Using absolute coordinates, the client renders the mouse movements locally, which improves performance, especially if you are outside the corporate network.

For work that requires using graphics-intensive applications, such as AutoCAD, or for playing 3D video games, you can improve mouse performance by enabling the relative mouse feature, which uses relative, rather than absolute, coordinates.

When the relative mouse feature is enabled, performance might be slow if you are outside the corporate network, on a WAN.

Prerequisites

A Horizon administrator must turn on 3D rendering for the desktop pool. For information about pool settings and the options available for 3D rendering, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

1. Start Horizon Client and log in to the server.
2. Right-click the remote desktop and select **VMware Blast** or **PCoIP**.
3. Connect to the remote desktop.
4. From the Settings dialog box, toggle the **Enable Relative Mouse** option to on.

   To disable the relative mouse feature, toggle the **Enable Relative Mouse** option to off.

   Note If you use Horizon Client in windowed mode rather than full-screen mode and the relative mouse feature is enabled, you might not be able to move the mouse pointer to the Horizon Client menu options or move the pointer outside of the Horizon Client window. To resolve this situation, press Ctrl+Alt.

Using Scanners

With the scanner redirection feature, you can scan information into remote desktops and published applications with scanners that are connected to the local client system. This feature redirects scanning data with a significantly lower bandwidth than can be achieved by using USB redirection.

Scanner redirection supports standard scanning devices that are compatible with the TWAIN and WIA (Windows Image Acquisition) formats. You must install the scanner device drivers on the local client system. You do not need to install the scanner device drivers on a remote desktop.

If a Horizon administrator has configured the scanner redirection feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, a scanner connected to your local client system can be used in a remote desktop or published application.

Important Do not connect a scanner from the **Connect USB Device** menu in Horizon Client. The performance will be unusable.

When scanning data is redirected to a remote desktop or published application, you cannot access the scanner on the local client computer. Conversely, when a scanner is in use on the local client computer, you cannot access it on the remote desktop or published application.

A Horizon administrator can configure group policy settings to control the options that available in the VMware Horizon Scanner Redirection Preferences dialog box. For more information, see the *Configuring Remote Desktop Features in Horizon* document.

Note If a Horizon administrator configures scanner redirection to use a specific scanner and that scanner is not available, scanner redirection does not work.

Tips for Using the Scanner Redirection Feature

- To change scanner redirection settings, click the scanner icon (🖼) in the system tray or notification area of the remote desktop. In a published application, the system tray icon is redirected to the local client computer.

  Note You do not need to use the menu that appears when you click the scanner icon. Scanner redirection works without any further configuration. If the menu does not list any scanners, an incompatible scanner is connected to the local client system. If the scanner icon does not appear, the scanner redirection feature is either disabled or not installed on the remote desktop. The scanner icon also does not appear on local client systems that do not support this feature.

- If you want the TWAIN Scanning Properties dialog box to appear even if a scanning application does not display the scanning dialog box, click the **Preferences** option in the scanner icon menu and select the **Force the TWAIN Scanning Properties dialog** check box.
- To display the actual scanner names rather than VMware Virtual *nnn* scanner, click the **Preferences** option in the scanner icon menu and select the **Use vendor defined names for TWAIN scanners** check box.
- To select options to control image compression or determine how to select the default scanner, click the **Preferences** option in the scanner icon menu and select the **Compression** or **Defaults** tab.
- If you plan to use the Real-Time Audio-Video feature to redirect webcams as recommended by VMware, click the **Preferences** option in the scanner icon menu and select the **Hide webcam type imaging devices** check box.

- Most TWAIN scanners display a scanner settings dialog box by default, but some do not. For those scanners that do not display settings options, you can use the **Preferences** option in the scanner icon menu and select the **Force the TWAIN Scanning Properties dialog** option.
- To display the TWAIN Scanner Properties dialog box on the remote desktop, click the **Preferences** option in the scanner icon menu and select the **Agent (VMware Scanning Properties dialog)** check box. To display the TWAIN Scanner Properties dialog box on the local client system, select the **Client (Native Scanning Properties dialog, if supported)** check box.

  Note In the agent-side TWAIN Scanner Properties dialog box, some less-common options might not be included. To use these less-common options, select the **Client (Native Scanning Properties dialog, if supported)** check box.
- Scanning too large an image or scanning at too high a resolution might not work. In this case, you might see the scanning progress indicator freeze, or the scanner application might exit unexpectedly. If you minimize the remote desktop, an error message might appear on the local client system, notifying you that the resolution is set too high. To resolve this issue, reduce the resolution or crop the image to a smaller size and scan again.

Redirecting Serial Ports

With the serial port redirection feature, you can redirect locally connected serial (COM) ports, such as built-in RS232 ports and USB-to-serial adapters. Devices such as printers, bar code readers, and other serial devices can be connected to these ports and used in remote desktops.

If a Horizon administrator has configured the serial port redirection feature, and if you use the VMware Blast display protocol or the PCoIP display protocol, serial port redirection works in the remote desktop without further configuration. For example, COM1 on the local client system is redirected as COM1 on the remote desktop. COM2 is redirected as COM2. If the COM port is already in use, it is mapped to avoid conflicts. For example, if COM1 and COM2 exist on the remote desktop, COM1 on the client system is mapped to COM3 by default.

You must have any required device drivers installed on the local client system, but you do not need to install the device drivers on the remote desktop. For example, if you use a USB-to-serial adapter that requires specific device drivers to work on your local client system, you must install those drivers, but only on the client system.

Important If you are using a device that plugs in to a USB-to-serial adapter, do not connect the device from the **Connect USB Device** menu in Horizon Client. Doing so routes the device through USB redirection and bypasses the serial port redirection feature.

Tips for Using the Serial Port Redirection Feature

- Click the serial port icon ( ) in the system tray or notification area of the remote desktop to connect, disconnect, or customize the mapped COM ports.

When you click the serial port icon, the **Serial COM Redirection for VMware Horizon** context menu appears. If an administrator has locked the configuration, the items in the context menu are dimmed. The icon appears only if a Horizon administrator has configured the serial port redirection feature and all requirements are met. For more information, see System Requirements for Serial Port Redirection.

- In the context menu, the port items are listed as ***port* mapped to *port***, for example, **COM1 mapped to COM3**. The first port, which is COM1 in this example, is the physical port or the USB-to-serial adapter on the local client system. The second port, which is COM3 in this example, is the port used in the remote desktop.
- To select the **Port Properties** command, right-click a COM port.

  In the COM Properties dialog box, you can configure a port to connect automatically when a remote desktop session is started, or you can ignore DSR (data-set-ready signal), which is required for some modems and other devices.

  You can also change the port number that the remote desktop uses. For example, if the COM1 port on the client system is mapped to COM3 in the remote desktop, but the application you are using requires COM1, you can change the port number to COM1. If COM1 exists in the remote desktop, you might see **COM1 (Overlapped)**. You can still use this overlapped port. The remote desktop can receive serial data through the port from the server and also from the client system.
- Connect to a mapped COM port before you attempt to start an application that requires access to the port. For example, right-click a COM port and select **Connect** to use the port in the remote desktop. When you start the application, the application opens the serial port.

  When a redirected COM port is opened and in use on a remote desktop, you cannot access the port on the local computer. Conversely, when a COM port is in use on the local computer, you cannot access the port on the remote desktop.
- In the remote desktop, you can use the Windows Device Manager **Port Settings** tab to set the default Baud rate for a particular COM port. Use the same settings in the Windows Device Manager on the client system. The settings from this tab are used only if the application does not specify the port settings.
- Before you can disconnect the COM port, you must close the port in the application or close the application. You can then select the **Disconnect** command to disconnect and make the physical COM port available for use on the client computer.
- If you configure a serial port to connect automatically, start an application that opens the serial port, and then disconnect and reconnect the remote desktop session, the auto-connect feature does not work. You also cannot connect by using the serial port's system tray icon's menu option. In most cases, the application can no longer use the serial port. You must stop the application, disconnect the remote desktop session, and reconnect again to resolve the problem.

Keyboard Shortcuts for Input Focus

You can use the **Hotkey combination to grab input focus** and **Hotkey combination to release input focus** group policy settings to configure keyboard shortcuts for input focus.

You can use the **Automatic input focus in a virtual desktop window** group policy setting to send input to the remote desktop automatically when a user brings the remote desktop to the front. These features are useful for users who cannot use mouse clicks to grab and release a remote desktop. For more information, see Using Group Policy Settings to Configure Horizon Client.

Keyboard Input Source Language Synchronization

When you connect to a remote desktop, the keyboard input source language on the client system is synchronized in the remote desktop.

This feature supports the following keyboard input source languages on the client system.

- English
- French
- German
- Japanese
- Korean
- Spanish
- Simplified Chinese
- Traditional Chinese

Synchronization does not occur if the keyboard input source language is not supported.

Keyboard input source language synchronization is controlled by the agent-side **Keyboard locale synchronization** group policy setting. For more information, see "VMware Blast Group Policy Settings" in the *Configuring Remote Desktop Features in Horizon* document.

Configure Lock Key Synchronization

You can configure Horizon Client to synchronize the toggle states of the Num Lock, Scroll Lock, and Caps Lock keys from the client system to a remote desktop by enabling a setting in Horizon Client. This setting is disabled by default.

You can also use the Horizon Client **Automatically synchronize the keypad, scroll and caps lock keys** group policy setting to configure lock key synchronization. When this group policy setting is enabled or disabled, users cannot change the lock key synchronization setting in the Horizon Client user interface. For more information, see Using Group Policy Settings to Configure Horizon Client.

If the **Automatically synchronize the keypad, scroll and caps lock keys** group policy setting is either disabled or not configured, or the Horizon Client lock key synchronization setting is not selected (the default setting), the lock key toggle state is synchronized from the remote desktop to the client system by default.

Procedure

1 Start Horizon Client and connect to a server.

2 Open the Settings dialog box for the remote desktop.

   - Click the **Settings** (gear) icon in the upper-right corner of the desktop and application selection window and select the remote desktop in the left pane.
   - Right-click the remote desktop in the desktop and application selection window and select **Settings**.

3 To enable the lock key synchronization feature, toggle the **Automatically synchronize the keypad, scroll and caps lock keys** option to on.

Troubleshooting Horizon Client 6

You can solve most problems with Horizon Client by restarting or resetting remote desktops or published applications, or by reinstalling Horizon Client.

This chapter includes the following topics:

- Restart a Remote Desktop
- Reset Remote Desktops or Published Applications
- Repair Horizon Client for Windows
- Uninstall Horizon Client for Windows
- Problems with Keyboard Input
- What to Do If Horizon Client Quits Unexpectedly
- Connecting to a Server in Workspace ONE Mode

Restart a Remote Desktop

If the remote desktop operating system stops responding, you might need to restart a remote desktop. Restarting a remote desktop is similar to using the Windows operating system restart command. The remote desktop operating system usually prompts you to save any unsaved data before it restarts.

You can restart a remote desktop only if a Horizon administrator has enabled the restart feature for the remote desktop and the remote desktop is powered on. You can restart only one remote desktop at a time.

For information about enabling the desktop restart feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

- Use the **Restart Desktop** command.

Option	Action
From within the remote desktop	Select **Options** > **Restart Desktop** from the menu bar.
From the desktop selector window	Right-click the remote desktop icon and select **Restart Desktop**.

Horizon Client prompts you to confirm the restart action.

Results

The operating system in the remote desktop restarts and the client disconnects and logs off from the remote desktop.

What to do next

Wait an appropriate amount of time for the system to restart before you attempt to reconnect to the remote desktop.

If restarting the remote desktop does not solve the problem, you might need to reset the remote desktop. See Reset Remote Desktops or Published Applications.

Reset Remote Desktops or Published Applications

You might need to reset a remote desktop if the desktop operating system stops responding and restarting the remote desktop does not solve the problem.

Resetting a remote desktop is the same as pressing the Reset button on a physical PC to force the PC to restart. Any files that are open on the remote desktop are closed and are not saved.

Resetting published applications quits all open applications.

You can reset a remote desktop only if a Horizon administrator has enabled the reset feature for the remote desktop and the remote desktop is powered on. You can reset only one remote desktop at a time.

For information about enabling the desktop reset feature, see the *Setting Up Virtual Desktops in Horizon* or *Setting Up Published Desktops and Applications in Horizon* document.

Procedure

1 To reset a remote desktop, use the **Reset Desktop** command.

Option	Action
From within the remote desktop	Select **Options** > **Reset Desktop** from the menu bar.
From the desktop and application selector window	Right-click the remote desktop icon and select **Reset Desktop**.

2 To reset published applications, use the **Reset** button in the desktop and application selector window.

   a Click the **Settings** button (gear icon) in the menu bar.

   b Select **Applications** in the left pane, click the **Reset** button in the right pane, and click **OK**.

Results

When you reset a remote desktop, the operating system in the remote desktop restarts and the client disconnects and logs off from the remote desktop. When you reset published applications, the published applications quit.

What to do next

Wait an appropriate amount of time for system to restart before attempting to reconnect to the remote desktop or published application.

Repair Horizon Client for Windows

Sometimes you can resolve problems with Horizon Client by repairing Horizon Client.

Prerequisites

- Verify that you can log in as an administrator on the client system.
- Verify that you have the Horizon Client installer. You cannot repair Horizon Client if you do not have the installer.

Procedure

- To repair Horizon Client interactively, perform one of the following tasks.
  - Double-click the Horizon Client installer and click **Repair**.
  - Run the Horizon Client installer from the command line and enter the `/repair` command.

    For example, at the command prompt, type the following command:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
    ```

    y.y.y is the version number and *xxxxxx* is the build number.
- To repair Horizon Client silently, run the Horizon Client installer from the command line and enter the `/silent` and `/repair` commands.

  For example, at the command line, type the following command:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair
  ```

  y.y.y is the version number and *xxxxxx* is the build number.

Uninstall Horizon Client for Windows

If repairing Horizon Client does not solve the problem, you might need to uninstall and reinstall Horizon Client.

This procedures shows you how to uninstall Horizon Client when you have the Horizon Client installer.

If you do not have the Horizon Client installer, you can uninstall Horizon Client in the same way that you uninstall other applications on your Windows system. For example, on a Windows 10 system, you can use the Windows operating system uninstall or change a program feature (**Control Panel > Programs and Features > Uninstall or change a program**).

Prerequisites

Verify that you can log in as an administrator on the client system.

Procedure

- To uninstall Horizon Client interactively, perform one of the following tasks.
  - Double-click the Horizon Client installer and click **Remove**.
  - Run the Horizon Client installer from the command line and enter the `/uninstall` command.

    For example, at the command prompt, type the following command:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
    ```

    y.y.y is the version number and *xxxxxx* is the build number.
- To uninstall Horizon Client silently, run the Horizon Client installer from the command line and enter the `/silent` and `/uninstall` commands.

  For example, at the command prompt, type the following command:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall
  ```

  y.y.y is the version number and *xxxxxx* is the build number.

What to do next

Reinstall Horizon Client. See Chapter 2 Installing and Upgrading Horizon Client for Windows.

Problems with Keyboard Input

When you type in a remote desktop or published application, none of the keystrokes seem to work.

Problem

When you are connected to a remote desktop or published application, no characters appear when you type. Another symptom might be that a single key keeps repeating itself.

Cause

Some security software, such as Norton 360 Total Security, includes a feature that detects keystroke logging software and blocks keystroke logging. This security feature is meant to protect the system against spyware that steals passwords and credit card numbers. This security software might block Horizon Client from sending keystrokes to the remote desktop or published application.

Solution

- ◆ On the client system, turn off the keystroke logging detection feature of your antivirus or security software.

What to Do If Horizon Client Quits Unexpectedly

Horizon Client quits even if you do not close it.

Problem

Horizon Client quits unexpectedly. Depending on the server configuration, you might see a message such as `There is no secure connection to the View Connection Server`. Sometimes a message does not appear.

Cause

This problem occurs when the connection to the server is lost.

Solution

- ◆ Restart Horizon Client. You can connect successfully when the server is running again. If you continue to have connection problems, contact your system administrator or VMware Support.

Connecting to a Server in Workspace ONE Mode

You cannot connect to a server directly through Horizon Client, or your remote desktop and published application entitlements are not visible in Horizon Client.

Problem

- When you try to connect to the server directly through Horizon Client, Horizon Client redirects you to the Workspace ONE portal.
- When you open a remote desktop or published application through a URI or shortcut, or when you open a local file through file association, the request redirects you to the Workspace ONE portal for authentication.

- After you open a remote desktop or published application through Workspace ONE and Horizon Client starts, you cannot see or open other entitled remote desktops or published applications in Horizon Client.

Cause

A Horizon administrator can enable Workspace ONE mode on a Connection Server instance. This behavior is normal when Workspace ONE mode is enabled on a Connection Server instance.

Solution

Use Workspace ONE to connect to a Workspace ONE enabled server and access your remote desktops and published applications.